

# DISRUPTER SERIES: WEARABLE DEVICES

---

## HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, MANUFACTURING,  
AND TRADE

OF THE

COMMITTEE ON ENERGY AND  
COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

---

MARCH 3, 2016

---

**Serial No. 114–125**



Printed for the use of the Committee on Energy and Commerce  
*energycommerce.house.gov*

---

U.S. GOVERNMENT PUBLISHING OFFICE

20–248 PDF

WASHINGTON : 2016

---

For sale by the Superintendent of Documents, U.S. Government Publishing Office  
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800  
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

## COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan

*Chairman*

JOE BARTON, Texas

*Chairman Emeritus*

ED WHITFIELD, Kentucky

JOHN SHIMKUS, Illinois

JOSEPH R. PITTS, Pennsylvania

GREG WALDEN, Oregon

TIM MURPHY, Pennsylvania

MICHAEL C. BURGESS, Texas

MARSHA BLACKBURN, Tennessee

*Vice Chairman*

STEVE SCALISE, Louisiana

ROBERT E. LATTA, Ohio

CATHY McMORRIS RODGERS, Washington

GREGG HARPER, Mississippi

LEONARD LANCE, New Jersey

BRETT GUTHRIE, Kentucky

PETE OLSON, Texas

DAVID B. McKINLEY, West Virginia

MIKE POMPEO, Kansas

ADAM KINZINGER, Illinois

H. MORGAN GRIFFITH, Virginia

GUS M. BILIRAKIS, Florida

BILL JOHNSON, Ohio

BILLY LONG, Missouri

RENEE L. ELLMERS, North Carolina

LARRY BUCSHON, Indiana

BILL FLORES, Texas

SUSAN W. BROOKS, Indiana

MARKWAYNE MULLIN, Oklahoma

RICHARD HUDSON, North Carolina

CHRIS COLLINS, New York

KEVIN CRAMER, North Dakota

FRANK PALLONE, Jr., New Jersey

*Ranking Member*

BOBBY L. RUSH, Illinois

ANNA G. ESHOO, California

ELIOT L. ENGEL, New York

GENE GREEN, Texas

DIANA DeGETTE, Colorado

LOIS CAPPS, California

MICHAEL F. DOYLE, Pennsylvania

JANICE D. SCHAKOWSKY, Illinois

G.K. BUTTERFIELD, North Carolina

DORIS O. MATSUI, California

KATHY CASTOR, Florida

JOHN P. SARBANES, Maryland

JERRY McNERNEY, California

PETER WELCH, Vermont

BEN RAY LUJAN, New Mexico

PAUL TONKO, New York

JOHN A. YARMUTH, Kentucky

YVETTE D. CLARKE, New York

DAVID LOEBSACK, Iowa

KURT SCHRADER, Oregon

JOSEPH P. KENNEDY, III, Massachusetts

TONY CARDENAS, California

---

## SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND TRADE

MICHAEL C. BURGESS, Texas

*Chairman*

LEONARD LANCE, New Jersey

*Vice Chairman*

MARSHA BLACKBURN, Tennessee

GREGG HARPER, Mississippi

BRETT GUTHRIE, Kentucky

PETE OLSON, Texas

MIKE POMPEO, Kansas

ADAM KINZINGER, Illinois

GUS M. BILIRAKIS, Florida

SUSAN W. BROOKS, Indiana

MARKWAYNE MULLIN, Oklahoma

FRED UPTON, Michigan (*ex officio*)

JANICE D. SCHAKOWSKY, Illinois

*Ranking Member*

YVETTE D. CLARKE, New York

JOSEPH P. KENNEDY, III, Massachusetts

TONY CARDENAS, California

BOBBY L. RUSH, Illinois

G.K. BUTTERFIELD, North Carolina

PETER WELCH, Vermont

FRANK PALLONE, Jr., New Jersey (*ex officio*)

## C O N T E N T S

	Page
Hon. Michael C. Burgess, a Representative in Congress from the State of Texas, opening statement .....	1
Prepared statement .....	3
Hon. Frank Pallone, Jr., a Representative in Congress from the State of New Jersey, opening statement .....	4
Hon. Janice D. Schakowsky, a Representative in Congress from the State of Illinois, opening statement .....	5
WITNESSES	
Thomas D. Bianculli, Vice President, Enterprise Technology Office, Zebra Technologies .....	6
Prepared statement .....	9
Answers to submitted questions .....	80
Meg Burich, Director of Commercial Development and Marketing, Adidas Digital Sports .....	16
Prepared statement .....	18
Answers to submitted questions <sup>1</sup> .....	86
Suresh Palliparambil, American Sales and Business Development Director, NXP .....	21
Prepared statement .....	24
Answers to submitted questions .....	87
Scott Peppet, Professor of Law, University of Colorado School of Law .....	29
Prepared statement .....	32
Answers to submitted questions <sup>1</sup> .....	91
Doug Webster, Vice President, Service Provider Marketing, Cisco .....	43
Prepared statement .....	45
Answers to submitted questions .....	92
SUBMITTED MATERIAL	
Letter of March 3, 2016, from Steven K. Berry, President and Chief Executive Officer, Competitive Carriers Association, to Mr. Burgess and Ms. Schakowsky, submitted by Mr. Burgess .....	58
Statement of Mercatus Center at George Mason University, by Adam Thierer, Senior Research Fellow, Technology Policy Program, March 3, 2016, submitted by Mr. Burgess .....	60

<sup>1</sup>Ms. Burich and Mr. Peppet did not answer submitted questions for the record by the time of printing.



## DISRUPTER SERIES: WEARABLE DEVICES

---

THURSDAY, MARCH 3, 2016

HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEE ON COMMERCE, MANUFACTURING, AND  
TRADE,  
COMMITTEE ON ENERGY AND COMMERCE,  
*Washington, DC.*

The subcommittee met, pursuant to call, at 10:02 a.m., in room 2123, Rayburn House Office Building, Hon. Michael C. Burgess (chairman of the subcommittee) presiding.

Members present: Representatives Burgess, Lance, Harper, Guthrie, Bilirakis, Brooks, Schakowsky, Kennedy, Welch, and Pallone (ex officio).

Staff present: Leighton Brown, Deputy Press Secretary; Rebecca Card, Assistant Press Secretary; James Decker, Policy Coordinator, Commerce, Manufacturing, and Trade; Graham Dufault, Counsel, Commerce, Manufacturing, and Trade; Melissa Froelich, Counsel, Commerce, Manufacturing, and Trade; Giulia Giannangeli, Legislative Clerk, Commerce, Manufacturing, and Trade; Paul Nagle, Chief Counsel, Commerce, Manufacturing, and Trade; Olivia Trusty, Professional Staff Member, Commerce, Manufacturing, and Trade; Dylan Vorbach, Deputy Press Secretary; Michelle Ash, Democratic Chief Counsel, Commerce, Manufacturing, and Trade; Christine Brennan, Democratic Press Secretary; Elisa Goldman, Democratic Counsel, Commerce, Manufacturing, and Trade; Caroline Paris-Behr, Democratic Policy Analyst; Diana Rudd, Democratic Legal Fellow; and Matt Schumacher, Democratic Press Assistant.

Mr. BURGESS. The Subcommittee on Commerce, Manufacturing, and Trade will now come to order.

I will recognize myself for 5 minutes for an opening statement.

### **OPENING STATEMENT OF HON. MICHAEL C. BURGESS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS**

And I do want to welcome all of our witnesses here today and welcome everyone to another installment of our Disrupter Series hearings. Today, we will examine wearable technologies and how they are disrupting traditional business processes and transforming ways that consumers can engage in commerce.

Last year, we held a hearing to examine the Internet of Things, a network of Internet-connected physical objects that gather information in realtime to predict circumstances, prevent problems, and create opportunities. That market has now matured, and wearable technologies have come to represent a growing segment within that

digital ecosystem of interconnected devices and their applications and platforms.

The defining characteristic of wearables is that they offer consumers and businesses access to realtime, highly personalized information through products and devices that are physically worn by the user. Many of us are familiar with fitness tracking bands on the market today. They gather information about an individual's physical activity, or lack thereof, and are intended to motivate users to improve their fitness, wellness, and health regimens.

While inspiring better fitness habits is a positive use of wearable technology, the societal and economic benefits of these products extends far beyond those applications. We are just beginning to see the potential of wearable technology across multiple economic sectors and industries, such as energy, health care, transportation, retail, professional sports, manufacturing, education, and others.

In manufacturing, for example, wearables can provide businesses with greater insight into the daily operations of their production practices, their workflows, their supply chain processes.

In sports, coaches and athletic trainers can use wearables to better assess player recovery time and inform return-to-play considerations to reduce the risk of further injury. I just think back to my own brief high school sports career. The coach would know if I was dogging it realtime. He wouldn't have to accuse me; he would have the data.

In the automotive sector, wearable technology can sense early signs of driver fatigue, prompting the wearable device or vehicle to send alerts or another type of warning to the driver.

And in the retail industry, retailers can use wearable technology to customize product offerings and better meet consumer preferences and demand.

The appeal of this technology is pervasive because of what it can offer in terms of operational efficiencies, public safety, improved performance, and cost savings for every business type and size. The potential for wearable technology is virtually limitless.

Much of the excitement surrounding wearables is rooted in the promise to create new opportunities for economic growth, economic development, and job creation. Wearables create economic opportunities by providing insights into an individual's behavior and driving changes to that behavior to improve job performance and job execution. This can lead to increased productivity and efficiency, helping a business reduce waste and optimize resources.

The technology also facilitates smarter decisionmaking, increased information-sharing, and augmented interactions amongst workers. The productivity gains achieved through these operational advances are fundamental to a stronger and more prosperous economy.

As with all connected technologies, there are important privacy and security considerations that should be part of today's discussions. Unlike other connected things within the Internet of Things, such as connected thermostats, streetlights, and refrigerators, wearables are physically worn by users and capable of extracting highly personalized information about an individual's activities or whereabouts.

In our examination of these issues, it will be important to understand how consumers are using these technologies and how they will be protected while preserving the flexibility and the ingenuity of the innovators that are driving this market forward.

Once again, I want to thank our witnesses for taking the time to inform us about the applications and future potential.

I recognize the gentleman from New Jersey, 5 minutes for an opening statement, please.

[The prepared statement of Mr. Burgess follows:]

#### PREPARED STATEMENT OF HON. MICHAEL C. BURGESS

Good morning and welcome to another installment of our Disrupter Series hearings. Today we will examine wearable technologies and how they are disrupting traditional business processes and transforming the ways that consumers engage in commerce.

Last year we held a hearing to examine the Internet of Things—a network of Internet-connected physical objects that gather information in real-time to predict circumstances, prevent problems, and create opportunities. As that market has matured, wearable technologies, or “wearables”, have come to represent a growing segment within that digital ecosystem of connected devices, applications, and platforms. The defining characteristic of wearables is that they offer consumers and businesses access to real-time, highly personalized information through products and devices that are physically worn by the user.

Many of us are familiar with the fitness tracking bands on the market today. They glean information about an individual’s physical activity habits, and are intended to motivate users to improve their fitness, wellness, and health regimens. While inspiring better fitness habits is a positive use of wearable technology, the societal and economic benefits of these products and devices extend far beyond those applications.

We are just beginning to see the potential of wearable technology across multiple economic sectors in industries such as energy, health care, transportation, retail, professional sports, manufacturing, education, and many others.

In manufacturing, for example, wearables can provide businesses with greater insight into the daily operations of their production practices, workflows, and supply chain processes. In sports, coaches and athletic trainers can use wearables to better assess player recovery time and inform return-to-play considerations to reduce the risk of further injury. In the automotive sector, wearable technology can sense early signs of driver fatigue, prompting the wearable device or vehicle to send alerts, haptic feedback, or another type of warning to the driver. And, in the retail industry, retailers can use wearable technology to customize product offerings and better meet consumer preferences and demand.

The appeal of this technology is so pervasive because of what it can offer in terms of operational efficiencies, public safety, improved performance, and cost savings for every business type and size. The potential for wearable technology is virtually limitless.

Much of the excitement surrounding wearables is rooted in their promise to create new opportunities for economic growth, development, and job creation. Wearables create economic opportunities by providing insights into an individual’s behavior and driving changes to that behavior to improve job performance and execution. This can lead to increased productivity and efficiency, helping businesses reduce waste, optimize resources, and enhance communications. The technology also facilitates smarter decision-making, increased information sharing, and augmented interactions among workers. The productivity gains achieved through these operational advancements are fundamental to a stronger and more prosperous economy.

As with all connected technologies however there are important privacy and security considerations that should be a part of today’s discussion. Unlike other connected things within the Internet of Things ecosystem, such as connected thermostats, street lights, and refrigerators, wearables are physically worn by users, and capable of extracting highly personalized information about an individual’s activities. In our examination of these issues, it will be important to understand how consumers using these technologies will be protected while preserving the flexibility and ingenuity of innovators that are driving this market forward.

I thank the witnesses for taking the time to inform us about the applications and future potential of wearable technology. I look forward to a thoughtful and engaging discussion.

Mr. BURGESS. I recognize the gentleman from New Jersey, 5 minutes for an opening statement, please.

**OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY**

Mr. PALLONE. Thank you, Mr. Chairman.

Today's hearing gives us an opportunity to look at a diverse and quickly developing field. Wearable technology, part of the broader Internet of Things, provides consumers with capabilities that would have seemed more like science fiction than reality only a decade ago.

Today, you can buy a wristband that measures UV exposure, helping you avoid sun damage, or a sensor that sticks to skin and teaches you how to stretch to alleviate back pain or smart shoes that give you directions through buzzes to their feet.

Researchers from WINLAB, the Wireless Information Network Laboratory at Rutgers University in my district, collaborated to design a wearable that could replace passwords for head-worn devices by authenticating the user by measuring the unique movements of the head in response to audio stimulus. WINLAB reports that the device can accurately tell that the right person is wearing it at a rate of over 95 percent through tiny movements of the head alone.

Many wearables measure biometric data, giving consumers access to a wealth of personal information. Not long ago, if someone wanted to know their heart rate, quality of sleep, and calories burned, they would have had to be hooked up to a roomful of equipment. Today, they can simply put on a small bracelet and have all of that information at their fingertips.

And these are amazing advancements, but with these new innovations come new vulnerabilities. For example, when a doctor measures your heart rate, that information is protected from unauthorized disclosure. Those privacy protections do not apply to the same information collected through most wearable devices. And there are no standards for encryption or other security measures to protect the data wearables collect.

Long and complicated user terms and agreements have further compounded the problem. Some include clauses saying that the data they collect belongs to the company, not to the user. Most of us do not read every online user agreement word for word, so many wearable users are surprised when they learn that they may not own their own data.

Whether by sale or by data breach, the release of personal information from wearables can have serious implications. Employers, credit agencies, and health insurers can all use the data collected from wearables to draw inferences that may have a negative effect on the user.

As with other Internet of Things products, by building in security from the beginning, manufacturers of wearables can more effectively prevent hackers from gaining access to a device or the data it collects. By building in privacy, consumers can have confidence



in these products and buy them knowing that highly personal information will not be shared without their consent.

So I look forward to discussing the many great innovations in wearable technology today, but with these innovations we must also devote serious attention to how we can better protect consumers and their personal information in this space. When privacy and security are made a priority, both businesses and consumers benefit.

I yield back, Mr. Chairman.

Mr. BURGESS. The Chair thanks the gentleman. The gentleman yields back.

The Chair would inquire of the gentlelady from Illinois if she wishes to make an opening statement.

Ms. SCHAKOWSKY. I have a short statement.

Mr. BURGESS. You are recognized for 5 minutes.

**OPENING STATEMENT OF HON. JANICE D. SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS**

Ms. SCHAKOWSKY. Thank you, Mr. Chairman. And I really apologize for being late. I thank you, and I thank our panel.

So wearable devices have taken off in the last couple of years. I am sure there are a lot of people in this room who are wearing a Fitbit or some similar device. I happen to have lost mine. It fell off the first week I got it, and I haven't replaced it.

Companies have developed numerous applications in medical testing and health monitoring. For consumers, wearables mean convenient collection of detailed data. There is clearly great potential here, but as I am sure has been said before—and I know Chairman Pallone did—we need to make sure the consumers fully understand what they are getting into.

Let's talk about health applications. When a hospital collects your health information, that personal data is protected by HIPAA. Your healthcare provider is not allowed to share that information with marketers or send it to your employers without your consent. However, those privacy protections don't apply to most wearable devices.

In addition, consumers have been surprised to find that they don't own the data collected through their devices. Last year, Lark, a company that created a sleep coaching wristband, stopped supporting its device and the related app. Lark's customers lost easy access to their data. At the same time, Lark's privacy policy stated that it could sell this personal information if it is acquired or goes bankrupt.

This matters to consumers, because some of the data they collect through wearable devices is very valuable. Minute-by-minute data from a fitness tracker can be enough to determine your gender, age, stress level. That is why it is vital for wearable device companies to adequately protect consumer information.

Last year, the Federal Trade Commission issued a report concluding that companies making these devices must adopt reasonable security measures. The FTC also recommended that Congress enact baseline consumer privacy legislation for such devices. In today's hearing, I would like to delve deeper into these privacy con-

cerns as we consider how today's laws must evolve to fit tomorrow's technology.

Here are some basic principles that I think we should start from. Consumers should be able to expect that a company collecting their personal data is protecting this personal data. Consumers need to be informed what, how, and when data is shared. In addition, they need to know if they may lose access to information they have collected through a wearable device. Technology is developing rapidly. We need to ensure consumer protection keeps pace.

With that in mind, I would like to welcome our panelists. Your testimony is important to informing this discussion.

I yield back.

Mr. BURGESS. The Chair thanks the gentlelady. The gentlelady yields back.

This concludes member opening statements. And the Chair would remind members that, pursuant to committee rules, all members' opening statements will be made part of the record.

We do again want to thank our witnesses for being here, for taking their time to testify before the subcommittee.

Today's witnesses will have the opportunity to give opening statements, followed by a round of questions from members. Our witness panel for today's hearing will include Mr. Thomas Bianculli, Vice President for Enterprise Technologies at Zebra Technologies—you guys got out of order—Meg Burich, Director of Commercial Development and Marketing for Adidas Digital Sports; Suresh—help me pronounce your last name.

Mr. PALLIPARAMBIL. Palliparambil.

Mr. BURGESS. Suresh, welcome to the hearing.

Mr. PALLIPARAMBIL. No problem.

Mr. BURGESS. The Director of Sales and Business Development for NXP; Mr. Scott Peppet, Professor of Law at the University of Colorado School of Law; and Mr. Doug Webster, Vice President for Service Provider Marketing at Cisco.

We do appreciate you all being here with us today.

We are in the middle of a vote on the floor, but, Mr. Bianculli, I think we have time if you would like to give your opening statement. Then we will take a brief recess and come back and resume.

You are recognized for 5 minutes, please.

**STATEMENTS OF THOMAS D. BIANCULLI, VICE PRESIDENT, ENTERPRISE TECHNOLOGY OFFICE, ZEBRA TECHNOLOGIES; MEG BURICH, DIRECTOR OF COMMERCIAL DEVELOPMENT AND MARKETING, ADIDAS DIGITAL SPORTS; SURESH PALLIPARAMBIL, AMERICAN SALES AND BUSINESS DEVELOPMENT DIRECTOR, NXP; SCOTT PEPPET, PROFESSOR OF LAW, UNIVERSITY OF COLORADO SCHOOL OF LAW; AND DOUG WEBSTER, VICE PRESIDENT, SERVICE PROVIDER MARKETING, CISCO**

#### **STATEMENT OF THOMAS D. BIANCULLI**

Mr. BIANCULLI. Thank you, Chairman Burgess, Ranking Member Schakowsky, and members of the subcommittee, for the opportunity to testify before you today.

I am the Vice President of the Emerging Technology Office at Zebra Technologies Corporation in Lincolnshire, Illinois. With nearly \$4 billion in annual revenue, Zebra is a global market leader in a number of advanced technologies, including the Internet of Things and the related area of wearable technology.

While many Americans may not recognize Zebra by name, they come into contact with our solutions every day. For example, the barcode labels that are prominently featured on airline bag tags, express delivery packages, and pharmaceutical prescription bottles are often generated by a Zebra barcode label printer and tracked and managed by Zebra scanners, mobile computers, and wireless infrastructure.

Our pioneering technology vision and trusted enterprise solutions, particularly our wearables that are the focus of today's hearing, are dedicated to helping business, Government, and nonprofits make smarter decisions and take smarter actions by providing them with realtime visibility and mission-critical information in an ever-more-efficient manner.

Zebra commends the subcommittee for hosting this series of hearings on technological disrupters. Mr. Chairman, I will stress five key points.

First, let me begin with Zebra's role in the wearable market. Zebra's leadership in this market derives from our recreation of the overall wearables product category nearly 25 years ago. With the launch of our wrist-mounted terminal and ring scanner in 1992, we invented the first handheld laser barcode scanner, the first barcode printer, and the first WiFi-enabled mobile computer. We remain at the very forefront of breakthrough innovation as we continue to create wearables that go from the wrist and hand, as you see before me, to lanyards and heads-up computing solutions.

Second, we commend the subcommittee for its recognition of the wearable category as a disrupter. Wearables earn this status because they empower workers with total hands-free mobility in a manner that also provides instant access to business-critical information.

Instead of needing multiple devices that are all directed by hand, wearables enable new levels of productivity by providing employees with tools that marry natural language interaction with immediately available information, be it visual, verbal, or augmenting the user's physical reality.

Imagine, Mr. Chairman, a simple verbal command that provides a worker with full access to data and subject matter expertise in realtime. Imagine, further, the same worker using another verbal command to respond back and transmit data or pictures to a main office, a remotely located colleague, or to another machine. Now imagine having that ability while suspended high above the ground repairing the electrical grid or working inside an aircraft, no hands required. Wearable technology makes it happen.

Third, I would like to offer a quick look into the future. Awareness and acceptance of smartphone technology has grown at a tremendous pace and has built the foundation for wearable device adoption. Current technologies will continue to evolve and revolutionize the way people instinctively work with computers and intuitively interact with their virtual or augmented reality environ-

ments. It is not an overstatement to say that the possibilities of these devices are limitless.

Over the next few years, they will get smaller with technological improvements in computing, analytics, power, and display optics. As part of this trend, we will continue to advance our portfolio of wearables. We are presently focused on developing an augmented reality wearable system for true hands-free application, providing a future solutions approach for uninterrupted workflow and opening up the possibilities of what realtime, eye-level information can do.

Fourth, the economic benefits of wearables come from its significant impact on productivity across virtually every industry and economic sector. This is because visual computing or the ability to work hands-free while receiving eye-level information will drive a major paradigm shift in how we, as humans, directly interface with computers. Visual or hands-free computing will enable this kind of frictionless, uninterrupted workflow. Even a small increase in the efficiency of manufacturing or warehouse workers through wearables could bring a profound economic benefit to our economy.

Fifth and finally, we urge Congress and the administration to take a light touch where wearable technology is concerned, for the same reasons that many in industry as well as in Congress and the administration have advocated for a light regulatory approach to the Internet of Things.

The primary challenge is to allow for the rapid development, deployment, and subsequent advancement of wearables in a manner that simultaneously addresses concerns over data, security, and encryption. The goal is to encourage technologies which provide enhanced, secure, and realtime visibility and access to information in a way that empowers workers to undertake more effective and timely decisions and actions.

To this end, Mr. Chairman, Zebra stands ready work with the subcommittee inadvancing policies which keep the United States at the leading edge of this exciting technology. And I again thank you for the opportunity to provide our views on wearables, and I look forward to your questions.

[The prepared statement of Mr. Bianculli follows:]

Testimony of

Thomas D. Bianculli  
Vice President, Emerging Technology Office

Zebra Technologies Corporation

Before the Subcommittee on Commerce, Manufacturing & Trade  
Committee on Energy & Commerce  
U.S. House of Representatives

March 3, 2016

Thank you, Chairman Burgess, Ranking Member Schakowsky and members of the Subcommittee, for the opportunity to testify before you today. My name is Tom Bianculli and I am the Vice President of the Emerging Technology Office at Zebra Technologies Corporation. With nearly \$4.0 billion in annual revenue, Zebra is a global market leader in a number of advanced technologies, including the Internet of Things (IoT) and the related area of wearable technologies.

While many Americans may not recognize Zebra by name, they come into contact with our solutions every day. For example, the barcode labels that are prominently featured on airline bag tags, express delivery packages, and pharmaceutical prescription bottles are often generated by a Zebra barcode label printer, and tracked and managed by Zebra scanners, mobile computers and wireless infrastructure. Avid skiers experience less time in lift lines because of Zebra RFID tags that are embedded in the lift tickets which enable resort operators to quickly move skiers through waiting lines. Retail shoppers see our tags on clothing as an inventory management tool that enables stores to have the right products available on the shelves in real time. Our pioneering technology vision and trusted enterprise solutions, particularly our wearable technologies that are the focus of today's hearing, are dedicated to helping business, government

and non-profits make smarter decisions and take smarter actions by providing them with real-time visibility and mission-critical information in an ever more efficient manner.

Zebra commends the Subcommittee for hosting this series of hearings on technological disrupters. America's future technological leadership is best expressed in our ability to continually upend and overturn existing technological and business models; and wearable technologies are a key example of how this remarkable capability continues to express itself in our economy.

Wearable technologies have long been the stuff of science fiction. In 1931, author and cartoonist Chester Gould introduced America to super-detective Dick Tracy and his 2-way wrist radio. Later, in the 1960s, Gene Roddenberry provided us with an early glimpse of 21<sup>st</sup> century technology through the devices we saw in each episode of Star Trek. Since then, technologies that were once portrayed as futuristic in movies and television have come to life and have set the stage for the technological disruption that the Subcommittee is now studying.

In the interests of time, Mr. Chairman, I will quickly stress five key points that I will be pleased to detail further during the question and answer period that follows the panel.

- First, Zebra's role in the wearable technology market,
- Second, why wearable technology is a disrupter,
- Third, what the future holds in wearable technology,
- Fourth, the economic benefits of wearable technology, and
- Fifth, what we would urge Congress and the Administration to consider in terms of policy.

**Zebra's Role in the Wearable Technology Market**

Let me begin with Zebra's role in the wearable technology market. Much like our role with other Internet of Things (IoT)-related technologies, Zebra's leadership in the wearable technology market derives from our creation of the overall wearable technology product category nearly twenty-five years ago with the launch of our wearable wrist mounted terminal and finger ring scanner in 1992. We invented the first hand held laser barcode scanner, the first barcode printer, and the first miniature scan engine. We remain at the very forefront of breakthrough innovation in this space as we continue to create wearable technologies that go from the wrist and hand to lanyards and heads-up computing solutions. For example, many in industry are well aware of our hands-free head-mounted computer, the HC1, which was first launched in 2013. Our entire wearable tech line leverages the deep knowledge and insight gained from our unique and extensive industry experience.

**Why Wearable Technology is a Disrupter**

Second, we commend the Subcommittee for its recognition of the wearable category as a disrupter technology. Wearables earn this status because they empower workers with total hands-free mobility in a manner that also provides instant access to business-critical information. Instead of needing multiple devices that are all directed by hand, wearable technology enables new levels of productivity by providing employees with tools that marry natural language interaction with immediately available information be visual, verbal or augmenting the user's physical reality.

With wearable technology, workers can instantly access and view essential documents and complex schematics with just a simple voice command or turn of the head. No hands, no

laptop nor any fixed mobile workstation is required to get a complex task completed. The savings in time, performance and accuracy are dramatic. Whether it's fixing machines in a manufacturing setting or treating patients, wearables are becoming ever more adaptable in their ability to add significant value and assistance to workforces and emergency responders in times of need.

What this means is that performance will be improved and cycle time will be reduced as wearable technology provides enhanced situational awareness by giving people real-time access to critical data and video at the point of work. Again, Mr. Chairman, imagine a simple verbal command that provides a worker with full access to business critical data and subject matter experts in real-time. Imagine, further, the same worker using another verbal command to respond back and transmit data or pictures to a main office, a remotely located colleague, or to another machine. Now imagine having that ability while suspended high above the ground repairing the electrical grid or working inside an airplane engine. No hands required. Wearable technology makes it happen.

#### **What the Future Holds**

Third, I'd like to offer a quick look into what the future holds. Awareness and acceptance of smartphone technology has grown at a tremendous pace and has built the foundation for wearable device adoption. Current technologies will continue to evolve and revolutionize the way people instinctively work with computers and intuitively interact with their virtual or augmented reality environments.

Greater mobility, miniaturization, and the need to stay continuously connected are all current drivers of the wearable technology trend. Simplicity of use and the ability to work



independently or in conjunction with other external devices will continue to be some of the overall factors which drive the emerging wearable devices market which will change the way our economy works. Soon, we will see helmets, eyewear, vests, gear and clothing with interconnected sensor systems using standard off-the-shelf components. These will eventually evolve into heavy-duty, rugged functionality with basic plug-and-play capabilities ready for use in extreme field conditions and fully capable of supporting mission-critical applications.

It is not an overstatement to say that the possibilities of future wearable devices are limitless. Over the next few years, wearable devices will get smaller with technological improvements in computing, analytics, power and display optics. It may be too early to see biologically embedded or implantable devices, but more integrated devices using sensors that can enhance, monitor or tap into body signs are on the horizon. Many companies will create their own wearable technologies, creating a variety of different technology platforms and user experiences. The use of standard protocols such as Bluetooth and Wi-Fi will enable more wearable devices and peripherals to more easily talk to each other.

As part of this trend, we will continue to advance our portfolio of wearable technologies. We are presently leading the development of a see-thru visual computing experience to create a new wearable display system for augmented reality enterprise applications. We are strategically investing in emerging technologies to create a wide and see-thru visual computing experience for practical enterprise use – continuously mindful of human factors, ergonomics, and user experience. We're focused on developing an augmented reality wearable technology system for true hands-free application – providing a future solutions approach for uninterrupted workflow and opening up the possibilities of what real-time eye-level information can realistically do for business, government and non-profit users worldwide.

**The Economic Benefits Associated With Wearable Technology**

Fourth, the economic benefits of wearable technology come from its significant impact on productivity across virtually every industry and economic sector. This is because visual computing, or the ability to work hands-free while receiving eye-level information through wearable technology, will drive a major paradigm shift in how we, as humans, directly interface with computers. Visual, or hands-free, computing will enable this kind of frictionless, uninterrupted workflow. Even a small increase in the efficiency of manufacturing or warehouse workers through wearable technology could bring a profound economic benefit to our economy.

In a global economy which increasingly places a premium on compressed operational cycle times, dramatically reduced defect rates and ever-greater levels of workforce productivity, the impact of wearable technology will be significant as business, government and non-profits are better able to coordinate mission-critical and business-critical communications within and across organizations and make unlimited amounts of information available to individuals for better decision making.

**Policy Considerations**

Fifth, and finally, we urge Congress and the Administration to take a light touch where wearable technology is concerned – for the same reasons that many in industry as well as in Congress and the Administration have advocated for a light regulatory approach to the Internet of Things (IoT).

The primary challenge is to allow for the rapid development, deployment and subsequent advancement of wearable technology in a manner that simultaneously addresses concerns over

data security, encryption and privacy. In the ideal, the goal is to encourage technologies which provide enhanced, secure and real-time visibility and access to critical business information in a way that empowers employees and enables government, business, non-profits and individuals to undertake more effective and timely decisions and actions.

**Conclusion**

To this end, Mr. Chairman, Zebra stands ready to work with the Subcommittee in advancing policies which keep the United States at the leading-edge of this exciting technology and I, again, thank you for the opportunity to provide our views on wearable technology. I look forward to your and your colleagues' questions.

Mr. BURGESS. The Chair thanks the gentleman.

Because of the vote, we are going to go into recess.

Look, I want you all to know what you are up against with this congressional panel. Look at his notes, all stuck together and handwritten. You are down there with all of these fantastic technological devices, and we are kind of in the Stone Age.

But thank you for your forbearance. We are going to go vote. We will reassemble as soon as the last vote is over.

Mr. BIANCULLI. Thank you, Chairman.

[Recess.]

Mr. BURGESS. I thank everyone for their forbearance. The subcommittee will resume.

We will resume with the testimony of Ms. Meg Burich from Adidas Digital Sports.

#### STATEMENT OF MEG BURICH

Ms. BURICH. Good morning, Chairman and members of the subcommittee. Thank you for having me.

Mr. BURGESS. If I could just ask you if your microphone is on?

Ms. BURICH. It is on.

Ms. SCHAKOWSKY. Pull it a little more closer.

Ms. BURICH. Yes. OK. I am Meg Burich here on behalf of Adidas Digital Sports, and I am Director of Marketing and Commercial Development.

Adidas Digital Sports is the business unit within Adidas that drives the development of wearable technology. Our team consists of technology experts in the fields of data science, experience design, industrial design, algorithm development, software and hardware engineering. We have centers of excellence located in Portland, Oregon, Chadds Ford, PA, and Herzogenaurach, Germany where our headquarters is.

We have been active in the wearable space for over 15 years, with the first commercial launch of sensor-enabled footwear in 2001, and the introduction of real-time coaching under the Adidas miCoach brand in 2008. MiCoach offers real-time coaching to users, enabling them to achieve their goals by training with heart rate, speed, and distance to run faster and further.

Today, we are repositioning our wearables offering to address the growing opportunity for the larger population to benefit from this technology. All these products are enabled by companion software applications designed for mobile or desktop.

I am going to go through three examples to demonstrate the range of applications for wearables in sports, fitness, and health, and the first one will be related to schools and school children.

Adidas is partnering with Interactive Health Technologies to make fitness personal for kids in physical education classes. Instead of competing with each other, kids can wear an Adidas heart rate monitor that uses simple color zones to guide them through a fitness challenge. Wearable technology gives every kid the chance to know the good feeling that comes from a successful workout.

Next, I would like to cover the use of wearables in competitive and professional sports. We have a system. This is the jersey that athletes wear on the training field. Coaching software is coupled with this system, and coaches can see in real time what results are

coming from the athletes on the field. So instead of just driving them to train as hard as they can, they are really trying to train them in a smarter way, and in professional sports, there is kind of a fine line between peak performance and injury, so you want to really have this data to help you tell when you are really stressing an athlete versus when you are coaching him to the level where he can perform better.

Adidas uses in-depth experience with professional athletes and coaches to understand the cutting edge of performance. We also believe that all athletes and fitness participants deserve the best coaching, so we take what we learn working with the elite athletes, and then we translate that to smart systems for consumers, because consumers don't always have the option to hire a professional trainer. So we are making those consumer systems smart systems based on what we know about the cutting edge of coaching.

The third use case that I am going to go into focuses on women, and this is kind of a pivot for us in terms of how we see the market and the opportunity. Today, we know that women are managing their own health, and they have multi-generational influence. They are supporting healthcare decisions of their families and of their parents sometimes, so they are really kind of that officer of health.

These women are also the main users of fitness apps and devices. They are participating in digital social communities that help them stay engaged in their fitness routine. They may be going for a daily walk, getting ready for a 5K, or training for a marathon, but we have coaching solutions that will help them achieve their goal.

We have been talking a lot to women and researching their needs to understand what they are looking for, and basically, women are saying step counting is not enough. When they have a step counter, they either lose it or they drop it within 3 to 6 months. In fact, nearly 40 percent stop using it after 6 months. So we know they are looking for insights beyond how many steps they took. They really want the picture of their whole health, and managing it in a proactive way is important to them, so they are looking for tips on nutrition, they are looking for exercise tips, they are looking for guidance for how much to move during the day, how much they should sleep, and how that connects to their whole health and wellness.

So we know it is hard to stick to an exercise routine, and we are looking at how we can help women through digital wearables and digital experiences to stick with their exercise routine throughout their life, because we know that has an overall impact on health, disease prevention, and keeping people well. So we really believe that wearables is in its infancy, and wearables 2.0 is where we need to go, connecting consumers to health care and keeping them kind of on the wellness side. Thank you.

[The prepared statement of Ms. Burich follows:]

**WRITTEN TESTIMONY  
BEFORE THE COMMITTEE ON ENERGY AND COMMERCE**

**ADIDAS DIGITAL SPORTS**

adidas Digital Sports is the business unit within The adidas Group that drives the development of wearable technology. The Digital Sports Team consists of technology experts in the fields of data science, experience design, algorithm development and software and hardware engineering. We have centers of excellence located in Portland, OR, Chadds Ford, PA and Herzogenaurach Germany. adidas has been active in the wearable space for over 15 years with the first commercial launch of sensor enabled footwear in 2001 and the introduction of real time coaching under the adidas miCoach brand in 2008. miCoach offers real time coaching to users (ie – “speed up”, “slow down”...) enabling them to achieve their goals by training with heart rate, speed and distance to run further and faster. Today we are repositioning our Wearables offering to address the growing opportunity for the larger population to benefit from this technology. adidas holds an extensive patent portfolio in the space and offers a broad range of wearable products. All of these products are enabled by companion software applications designed for mobile and desktop use. This software is the key to making the information collected by a wearable understandable and actionable for the user.

To demonstrate the range of application for Wearables in sports, fitness and health we'll start with a use case that covers school children. adidas is partnering with Interactive Health Technologies to make fitness personal for kids in Physical Education Class. Instead of competing with each other, kids can wear an adidas heart rate monitor that uses simple color zones to guide them through a personal fitness challenge. Forget the awkward social situation that defined Gym Class of the past and often turned kids off to exercise from a young age.

Wearable technology gives every kid the chance to know the good feeling that comes from a successful workout. It teaches kids how to manage their own fitness and gives them a positive experience that sets them up to develop lifelong exercise habits.

Next I'd like to cover the use of Wearables in competitive and professional sports. Personalized training can be administered through Wearable Technology for those that are training to compete. Professional athletes and their coaches are using wearable technology to train. Coaching software coupled with sophisticated sensors in a base layer garment enables individuals and teams to optimize performance. Instead of a coach who drives the team to train as hard as they can and ultimately pushes past the optimum level, the coach can now guide athletes through a smart training program. With use of heart rate, accelerometers and GPS, coaches can see when an athlete is stressed and needs time to recover or when an athlete needs to put in more work. In the world of professional athletes there is a fine line between peak performance and injury. Giving coaches the ability to measure acceleration and heart rate and compare pre and post injury performance can help in return to play situations. In this case wearable technology is a tool for a coach to optimize the work he does with his players and keep them healthy throughout the season.

adidas uses in depth experience with professional athletes and coaches to understand the cutting edge of performance. We also believe that all athletes and fitness participants deserve the best coaching. Taking what we learn from elite and professional athletes and translating that to smart systems for consumers is a foundational design principle. Whether you play for the NBA or you're on the 7<sup>th</sup> grade basketball team, wearable technology can help you train at the right level for your individual situation. Wearable Technology coupled with well designed software applications can put the expertise of professional trainers, coaches and wellness experts in the

hands of the greater population who may not have access or the ability to afford these resources on their own.

The third use case focuses on women. Today we know that women are not only managing their own health, they have multi-generational influence. They are often supporting the health care decisions of their families and their aging parents. These women are the main users of fitness apps and devices. They participate in digital social communities that help them stay engaged in a fitness routine. Whether they are going for a daily walk, getting ready for their first 5K or training to run a marathon there's a Wearable that can help them achieve their goal. We've talked to women and researched their needs to understand why Wearables are often abandoned after 3 to 6 months of use. We know they are looking for insights beyond how many steps they took in a day. They want insights that address the picture of whole health including fitness, nutrition, mood and sleep. They are looking for Wearables that can connect the dots and keep them engaged in a healthy lifestyle.

We know it's hard to stick to an exercise routine. We also know that plenty of studies have shown the impact that exercise and an active lifestyle have on overall health, disease prevention and keeping people well. Through communities of Wearable users we are learning more and more about how to support active lifestyles and what works to keep people engaged in healthy fitness behaviors. Wearable Technology is no doubt an enabler in the early stages that can help people in their pursuit of a longer, healthier life.



Mr. BURGESS. The Chair thanks the gentlelady, and the Chair now recognizes Mr.—try again, Palliparambil.

Mr. PALLIPARAMBIL. You got it.

Mr. BURGESS. Five minutes.

Mr. PALLIPARAMBIL. Thank you.

Mr. BURGESS. Plus the 1 minute it took me to pronounce your name.

#### **STATEMENT OF SURESH PALLIPARAMBIL**

Mr. PALLIPARAMBIL. Thank you. Good morning, Chairman, and members of the committee. Thank you for holding this important hearing on wearable technologies today. My name is Suresh Palliparambil, and I am the America's Director of Sales and Business Development for NXP's secure identification solutions business line.

NXP helps to make today's ideas into tomorrow's exciting reality as the supplier of end-to-end solutions that range from semiconductor ICs to infrastructure components and secure applications.

We are the inventor of MIFARE and the co-inventor of NFC, the wireless proximity technology bringing new levels of simplicity and security to interactions of all kinds. NXP powers and enriches the IoT as a high-level contributor to standards bodies, including the FIDO Alliance, whose work promises to usher in a new era of on-line security, making the need to remember complex passwords a thing of the past.

As a proud employer of nearly 7,000 staff members in the U.S., NXP is committed to security leading-edge design and bringing products to the domestic market that have a substantial share of domestically built content and local value add to end products in which NXP plays a role.

Our company is dedicated to leveraging all of those resources and partnering with America's leaders to invest in the country's future and safer, more convenient lives for its citizens. From rockets in the air, to cars on the road, and cards in your wallet, our innovation at NXP has been integral to America's past and the success it enjoys today. As an important legacy as that is, we at NXP are looking to the future in building a better, easier, and safer tomorrow with exciting leading-edge technologies of utmost quality.

This is no small task. The rapid expansion of public and private data networks, the rise of social media, and the mass deployment of smart objects across the Internet of Things, IoT, have connected us in ways we didn't think possible two decades ago. They have also left us open, vulnerable, and exposed.

To counteract these vulnerabilities, NXP is focused on, one, avoiding unauthorized access in public and private areas of the IoT, developing tamper-resistant secure element devices, and perfecting the end-to-end solution that power the new, often wearable technologies will use to improve and simplify health care, entertainment, transportation, and the rest of our everyday lives.

Online security can mean different things to different people, but the task of keeping data private and ensuring cyber safety essentially comes down to one thing, access.

NXP has made authentication a top priority for more than 20 years and has continually reached new levels of performance by

making algorithms more resilient, and by increasing the robustness of secure elements. We are recognized as leaders in authentication, known for our ability to deliver trusted security in many of the world's most high-profile applications.

NXP produces chips that have their own unique fingerprint based upon their crystalline structure, so no two chips are alike, preventing cloning. NXP's strength in authentication is closely tied to eGovernment and banking. With roughly 80 percent market share of the electronic passport market, our technology is trusted by more national governments to increase security while reducing wait times at international borders. We are helping governments expand the use of electronic documents, and our repeated success with large-scale implementations of electronic IDs, public transportation, and multi-application cards, which combine payment, transportation, identification, and other services on a single card make a trusted partner to municipalities, transit authorities, and banking and payment organizations worldwide.

NXP brings a comprehensive set of skills to each authentication challenge and leverage outstanding relationship with broad spectrum of security leaders to develop and deliver tailored solutions that address needs in the market. The evolution in wearable technology is all about enhancing users' lives and making everyday functions simpler and easier so we can concentrate on the things that matter.

NXP creates the security, connectivity, and circuitry solutions that enable these wearable devices their convenient applications in today's society and the innovative ways they could be used in the future.

Many applications for wrist-based wearables are in place through entertainment venues and in the healthcare industry. The most popular example include keyless entry, smartwatches for luxury cars, Disney's RFID wristband, the MagicBand, an all-in-one device that serves as a room key, a park ticket to get in line, and also the payment, too.

There are already many existing areas where smartwatches could improve users' lives. Today's keyless entry for vehicles will probably move to a wearable platform, and in the future, watches will act as the key for an entire car. In fact, most luxury car makers already offer their own wristwatches. It is a great channel to help build their brand recognition.

In the home environment, smartwatches will interact with communication protocols such as ZigBee and Bluetooth, allowing users to control the home environment. Heating, lighting, AV equipment and more, will all be controlled by simply making a gesture with an arm or using apps installed on the watch. Soon, the smartwatch will be the only key anyone needs, the technology passport that gives access and control to your entire life.

NXP is working hard to simplify lives of citizens to secure transactions in the connected world, and we currently have the following tools and accomplishments in place to securely connect the next generation devices. We have a smart microcontroller platform; we have MIFARE, the world's leading contactless technology platform; Near Field Communications, which is a wireless proximity and

contactless technology; and then high-level contributions to standards bodies, including the FIDO Alliance for online security.

Thank you for the opportunity to participate in today's hearing. Thank you very much.

[The prepared statement of Mr. Palliparambil follows:]

## Wearables to Weather: NXP's Innovations for a Secure and Smarter Future

From rockets in the air, to cars on the road and the cards in your wallet, our innovations at NXP have been integral to America's past and the success it enjoys today. As important as that legacy is, however, we at NXP are looking to the future and building a better, easier and safer tomorrow with exciting, leading-edge technologies of the utmost quality.

This is no small task. The rapid expansion of public and private data networks, the rise of social media and the mass deployment of smart objects across the Internet of Things, or IOT, have connected us in ways we didn't think possible two decades ago. They've also left us open, vulnerable and exposed.

To counteract these vulnerabilities, NXP is focused on:

- ▶ Avoiding unauthorized access in public and private areas of the IoT,
- ▶ Developing tamper-resistant secure element devices, and
- ▶ Perfecting the end-to-end solutions that power the new, often wearable technologies we'll use to improve and simplify healthcare, entertainment, transportation and the rest of our everyday lives.

### Table of Contents

1	Overview	4	What's Next in Wearables
2	No authentication? No access.	4	Today's Wearables, Tomorrow's Next Big Things
2	Personal and Public Security	5	NXP and the Wearable Future
2	"Bulletproof" Authentication	5	The NXP Difference
3	NXP's Secure Elements		
3	NXP: Authentication Partner		



### No authentication? No access.

Online security can mean different things to different people, but the tasks of keeping data private and ensuring cyber safety essentially come down to one thing: **access**. Whenever there's a failure in security due to a data breach, a denial-of-service attack, identity theft, the spread of malware, or some other act of sabotage, the failure can almost always be tied to unauthorized access. At some point, someone found a way to be where they shouldn't have been, and did damage.

At its core, maintaining security is about preventing unauthorized access, and that means verifying the identity of anyone or anything requesting entry. Before being allowed to submit data, modify information, save settings, or execute tasks, a person, a device, or a piece of software must first verify that they are who they say they are. This process, known as **authentication**, is the starting point for all online security. When done right, authentication protects every interaction, and makes it safer for people, devices, and applications to access and share data. In the purely cyber realm, where operating systems and software code can interact on their own, effective authentication prevents intrusions, thefts and attempts to introduce viruses or malware. There is no better way to ensure the effectiveness of security protocols than to require people, devices and software to present a trusted identity.

### Personal and Public Security

No matter what the online scenario, authentication plays an essential role in keeping the process secure for everyone involved. For people using computers, smartphones, wearables, smartcards and electronic IDs to access services and exchange information, effective authentication ensures privacy while making purchases, logging onto a corporate network, riding public transport, updating health records, using government services, or simply sending an email.

In addition to individuals, industry and the government are often exposed to risk. For example, in his confirmation hearing, Ashton Carter, United States Secretary of Defense, stated that the Defense Department's network security "is not where it should be . . . [w]e're not anywhere near where we should be as a country . . . [n]ot only is our civilian infrastructure susceptible to cyberattack, but we have to be concerned about our military infrastructure."<sup>1</sup> For the rapidly growing IoT, effective authentication prevents criminals from accessing the data collected by devices or the software used to control device activity. This protects against the kinds of sabotage that can cripple the public infrastructure, which increasingly relies on smart grids and other network-controlled operations, and makes the IoT a safe place for private users, from the individual homeowner using a remotely-controlled thermostat to the global corporation or government managing thousands of connected devices.

### "Bulletproof" Authentication

Essentially, authentication is the manipulation of secret information through cryptographic algorithms to ensure security. The main challenge to effective, even "bulletproof," authentication is the aging of authentication algorithms. Previously secure systems become vulnerable as hackers and other criminals begin to erode the protection mechanisms. Data that was safe yesterday may not be safe today or tomorrow.

Staying ahead of the curve in terms of authentication involves two things: optimizing the algorithms to make them stronger, and creating better ways to protect the authentication process. The goal is to keep the data used for authentication inaccessible.

1. Yuhas, A. (2015). Pentagon pick Ashton Carter discusses Iraq and Ukraine at Senate hearing – as it happened. *The Guardian*. Retrieved from <http://www.theguardian.com/us-news/live/2015/feb/04/ashton-carter-senate-armed-services-committee-live>.

### NXP's Secure Elements

There are two aspects of authentication – the algorithms themselves and secure elements—tamper-resistant chip-based platforms that securely host an authentication algorithm and its confidential data. NXP's research indicates that in nearly all serious data breach cases, attackers extracted keys or credentials from devices or systems that offered no resistance. Our secure elements build on our groundbreaking work in microcontroller design, feature onboard countermeasures to protect from invasive, external attacks geared at data extraction, lead the industry in shipments and have earned a reputation for being many times more secure than their nearest competitors. For example, **NXP produces chips that have their own unique fingerprint, based upon their crystalline structure, so no two chips are alike, preventing cloning.**




### NXP: Authentication Partner

NXP has made authentication a top priority for more than 20 years, and has continually reached new levels of performance by making algorithms more resilient, and by increasing the robustness of secure elements. We are a recognized leader in authentication, known for our ability to deliver trusted security in many of the world's most high-profile applications.

NXP's strength in authentication is closely tied to eGovernment and banking. With a roughly 80 percent share of the electronic passport market, our technology is trusted by more national governments to increase security while reducing wait times at international borders. We are helping governments expand the use of electronic documents, and our repeated successes with large-scale implementations for electronic IDs, public transport, and multi-application cards (which combine payment, transport, identification, and other services on a single card), make us a trusted partner to municipalities, transit authorities, and banking and payment organizations worldwide. NXP brings a comprehensive set of skills to each authentication challenge and leverage long-standing relationships with a broad spectrum of security leaders to deliver tailored solutions that address the particular needs of each application.

Now that you've seen how NXP will keep the future of connected devices secure, let's take a look at the forefront of these connected technologies, their possibilities, and NXP's current and future role in developing and securing this tech for a brighter future.

### e-Government Applications

ELECTRONIC PASSPORT	NATIONAL ID	HEALTHCARDS
		
<b>Increased international border crossing security and efficiency</b> <ul style="list-style-type: none"> <li>▶ Higher security</li> <li>▶ Global Interoperability</li> <li>▶ ICAO compliance</li> <li>▶ Automated border crossing</li> </ul>	<b>Provide electronic identification &amp; enable governmental services</b> <ul style="list-style-type: none"> <li>▶ Higher security for personal authentication</li> <li>▶ Service cost and efficiency</li> </ul>	<b>Reduce healthcare costs via improved and efficient services</b> <ul style="list-style-type: none"> <li>▶ Patient identity</li> <li>▶ Electronic health records</li> <li>▶ Medication management</li> <li>▶ Enable social security services</li> </ul>

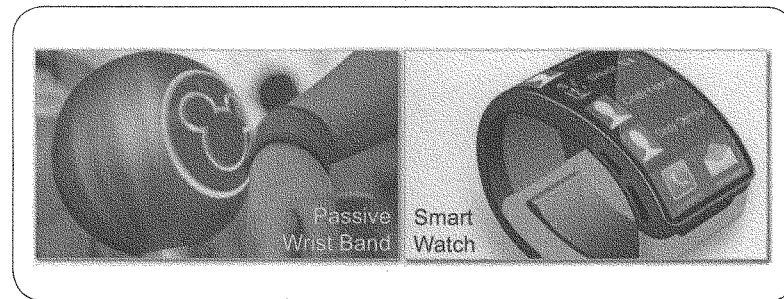
### What's Next in Wearables

Kazuo Kashio, the CEO of Casio, was quoted not long ago describing the human wrist as "prime real estate." Kazuo was alluding to the biggest technology battle that will take place in the next few years: the fight to dominate the wearable technology market. While there are a number of innovations taking place in the wearable technology space at the moment, with everything from smart glasses to intelligent hearing aids being developed, the competition probably will be fiercest around the wrist.

Previously, wristwear belonged exclusively to traditional watch manufacturers. Now technology companies are taking an interest in that "prime real estate" with the release of products like smart watches. Glancing down at a screen attached to the wrist is already such a natural action for many people. It's the reason why fitting someone's wrist with the latest tech in smart watches is so attractive for users and technology companies. While consumers will take some time adapting to devices such as smart glasses, strapping on the latest smartwatch is already seen as more of an upgrade that seamlessly blends smartphones and watches.

This evolution in wearable tech is all about enhancing users' lives and making everyday functions simpler and easier so we can concentrate on the things that matter. NXP creates the security, connectivity, and circuitry solutions that enable these wearables devices, their convenient applications in today's society and the innovative ways they could be used in the future.

### It's All in the Wrist



### Today's Wearables, Tomorrow's Next Big Things

To date, we've seen many smartwatch and other wrist-based innovations designed around fitness, health monitoring and entertainment. For example, Nike's FuelBand, the Fitbit and Jawbone products track steps, monitor heart rates and keep tabs on other vital information, all while synced to other smart devices.

Today's latest wrist-based tech innovation is not just limited to smartwatches. Walt Disney Parks and Resorts has unveiled its own RFID wrist tag application, the MagicBand. Walt Disney Parks and Resorts' MagicBands and cards are all-in-one devices that serve as guests' park tickets, room keys and more. The technology enables guests to book places on rides with the enhanced FastPass system FastPass+. RFID bracelets like the Disney MagicBand are increasingly being used for entrance and paying at other events with the tap of a wrist. It's simple, convenient movement that means no more lost cash at festivals.

### THE NXP DIFFERENCE

NXP powers and enriches the IoT as:

- The inventor of MIFARE, the world's leading technology for smartcard authentication
- The co-inventor of Near Field Communication (NFC), the wireless proximity technology bringing new levels of simplicity and security to interactions of all kinds
- A high-level contributor to standards bodies, including the FIDO Alliance, whose work promises to usher in a new era of online security, making the need to remember complex passwords a thing of the past.

### NXP and the Wearable Future

There are already many existing areas where smart watches could improve users' lives. Today's keyless entry for vehicles will probably move to a wearable platform, and in the future, watches will act as the key for the entire car. In fact, most luxury car makers already offer their own wrist watches. It's a great channel to help build brand recognition.

In the home environment, smartwatches will interact with communications protocols such as ZigBee and Bluetooth®, allowing users to control the home environment. Heating, lighting, AV equipment and more will all be controlled by simply making a gesture with an arm or using apps installed on the watch. Soon the smartwatch will be the only key anyone needs, the technology passport that gives access and control of your entire life.

Sensory data is also a rapidly growing market for wearable tech. Sensors built into a smartwatch or clothing will collect and process environmental factors such as humidity, pressure and temperature in addition to health data points. Everyone's local weather info can then be collated together and stored in the cloud to produce a micro-climate model. This would enable closer, more accurate measurement of air pollution and even plants could be watered automatically depending on conditions.

### The NXP Difference

NXP will help make these ideas into tomorrow's exciting reality as a supplier of end-to-end solutions that range from semiconductor ICs to infrastructure components and secure applications. We're the inventor of MIFARE, the world's leading technology for smartcard authentication, and the co-inventor of NFC, the wireless proximity technology bringing new levels of simplicity and security to interactions of all kinds.

As a proud employer of nearly 7,000 staff members in the United States, NXP is committed to security, leading-edge design, and bringing products to the domestic market that have a substantial share of domestically-built content and local value added to the end products in which NXP plays a role. Our company is dedicated to leveraging all of these resources and partnering with America's leaders to invest in this country's future and safer, more convenient lives for its citizens.

### How to Reach Us:

NXP Semiconductors USA, Inc.  
1455 Pennsylvania Avenue, NW, Suite 400,  
Washington, DC 20004  
Tel: +1.202.621.1831

[www.nxp.com](http://www.nxp.com)

NXP, the NXP logo, NXP SECURE CONNECTIONS FOR A SMARTER WORLD and MIFARE are trademarks of NXP B.V. All other product or service names are the property of their respective owners. © 2016 NXP B.V.



Mr. BURGESS. The Chair thanks the gentleman. Mr. Peppet, Professor Peppet, you are recognized for 5 minutes for your opening statement, please.

#### STATEMENT OF SCOTT PEPPET

Mr. PEPPET. Chairman Burgess, Ranking Member Schakowsky, members of the subcommittee, I appreciate the opportunity to talk to you about wearables. I am a Professor of Law at the University of Colorado Law School in Boulder, where I work on markets, technology, and privacy. I should say I am also a member of the board of directors of Anixter International, an Illinois-headquartered company, so my remarks today are in my own capacity, and in no way represent Anixter or anyone else.

I also want to say I am involved with four entrepreneurship and innovation centers: one in Colorado, one at Kellogg in Illinois, and one at the University of Michigan, and one actually in Israel at a university called IDC. And in that, in those roles, I have worked with student teams creating startups, many of whom are interested in or working in the wearable space. So I sort of got various perspectives on this set of issues.

These are exciting technologies, and I agree with my fellow witnesses who have said how much innovation is happening in this space, and I agree with all of that and just want to focus on three things in terms of privacy and security that I think deserve attention.

The first is one that you have already mentioned, which is data security, and I think there are two issues in data security. The first is, is the device itself secure? And that is a technical matter. Mostly, we know from research, that many of these devices have not been secured in the first wave of consumer devices, for example, and the reason is obvious: They are small, they are generally designed to be relatively inexpensive. It is hard to pack data security measures into a thing with a small processor, very limited connectivity, they are hard to update because they don't talk to the Internet that frequently.

And so it has been a challenge, and the FTC has worked with companies, continues to work to try to push companies in that space, or in the security issue, and I think we will see more innovation there to try to resolve some of those questions.

The second data security issue is actually not about the device, it is about the data. What happens to these data once they are off the device, they are stored in a company's cloud server somewhere, and someone hacks into that server. At the moment, if your credit card information is stolen from Target, for example, as you have all heard about that example, Target has to say, Hey, we were hacked, and they have to notify the public. That is our market-based response to data security in this country is to say, Listen, give consumers information, they will then choose with their dollars or their feet whether they want to go back to that store.

In all but one State, and Mr. Chairman, it is the great State of Texas, only Texas' data breach notification statute would actually apply to biometric data coming off of most of the wearables that we are talking about in the consumer space. The rest of the States really have not yet seen the risk that these incredibly sensitive

data, as you said, pose if they were to be hacked, which I think is an odd and sort of unfortunate anomaly.

To the extent that Congress ventures into the data breach notification area, that is something that it should consider. So that is security.

The second thing I will talk about is use, and I will just give a very simple example. There are lots of different devices at the moment being used in hospitals that keep track of whether a hospital worker washes his or her hands when they use the restroom. What they do is they have a lanyard on, you know, or some kind of ID badge, and there is a device at the sink and it literally just says how long did they spend standing in front of the sink? And then if they approach a hospital bed and they haven't washed their hands properly, their lanyard starts to buzz and say, hey, wait a minute, and it records that they have done that, and that is not a good thing.

That is a great idea, right? I think that is a terrific idea. I hope that every hospital I ever use has that, and employees, consumers, whoever we are talking about, need to know what those kinds of data are being used for. So for example, there might be no issue at all for a hospital or an employer using the data coming off a wearable for the obvious use that it was designed for, but I would guess that if one of the hospital employees discovered that their hand-washing habits had leaked out into data brokerages and was being used in credit decisions or insurance decisions or any other kind of decisions in the economy, they would be both surprised and unhappy. So the use issue is a very complicated one.

And the last one I will say something about is consent. Consent is hard, particularly in the consumer space, for these little devices. A study that I did, I brought 20 of these very popular devices, I opened all the boxes, and I looked inside. There is almost never any privacy information. I didn't test Adidas', but there is almost never privacy information in the box. Sometimes you get the privacy information when you download the app that pairs with the device. Often, you are sent to the Web site or you have to go to Web site of the firm, and often, when you get there and you read their privacy policy, it doesn't apply to the data coming off the device. It applies to the use of the Web site.

So at the moment, we are in a bit of a backward situation on how to give users and consumers, in particular, good information about these devices. Is the device information protected? Who owns the data? Can users go in and delete their data? Many have discovered that they can't, so their fitness data is being stored in the cloud somewhere and they say, I don't want to use this device anymore. They didn't just lose it. They affirmatively decided they don't like it anymore, and they say, I want to get my data back. I don't want you to have it anymore.

Many companies actually will not permit that or permit editing of this data. And most important, who is the data being shared with? Can it be sold in a bankruptcy, in an acquisition, or just in general?

So again, the FTC has been working with industry to try to come up with some guidance on those issues, but those consent questions are very difficult at the moment.

I will stop there. Thank you for allowing me to testify.  
[The statement of Mr. Peppet follows:]

Statement of Professor Scott Peppet  
Professor of Law, University of Colorado School of Law

Before the  
Subcommittee on Commerce, Manufacturing, and Trade  
Committee on Energy and Commerce  
U.S. House of Representatives

Hearing on Wearable Devices  
March 3, 2016

Very soon, we will see inside ourselves like never before, with wearable, even internal[,] sensors that monitor even our most intimate biological processes. It is likely to happen even before we figure out the etiquette and laws around sharing this knowledge.

-- Quentin Hardy, *The New York Times* (2012)<sup>1</sup>

Chairman Burgess, Ranking Member Schakowsky, and Members of the Subcommittee, I appreciate the opportunity to speak with you today about wearable technologies. I am a Professor of Law at the University of Colorado Law School, where my work focuses on technology, markets, and privacy. I am also a member of the Board of Directors of Anixter International Inc., a distributor of industrial cabling and technology components, which is involved in the creation of technology infrastructure although not directly involved in wearable technologies. My comments today are solely in my personal and academic capacity and in no way reflect the views of the Anixter corporation or other organizations with which I am affiliated.

Wearable technologies offer myriad benefits, including better health, increased productivity in the workplace, economic efficiencies, and higher quality of life. Encouraging continued innovation in this growing field is important: wearable technologies are

---

<sup>1</sup> Quentin Hardy, *Big Data in Your Blood*, Bits, N.Y. Times (Sept 7, 2012).

relatively new and we are only beginning to see their potential. At the same time, wearables create at least four risks that industry and lawmakers should monitor and work together to control: (1) new types of data security risks; (2) risk of context-violative uses of data produced by wearable devices; (3) de-anonymization or re-identification risks; and (4) the reality that consumers are not being afforded meaningful opportunities to consent to these risks.<sup>2</sup> By providing clear guidance on how to manage these four risks, lawmakers and regulators can ensure that consumers can trust wearable devices, thereby encouraging continued innovation in this growing industry.

#### I. Types of Wearables

It is important to recognize that wearable technology has already progressed far beyond simple electronic pedometers or fitness monitors. Wearables now include:

Fitness devices, such as:

- Fitness bracelets that can track steps taken, calories burned, minutes asleep, heart rate, and sometimes location<sup>3</sup>
- Bicycling helmets and baseball caps that can track heart rate and caloric consumption<sup>4</sup>
- Sensor-filled socks that can detect how far and fast a user runs as well as detect risk of injury<sup>5</sup>
- Bio-tracking clothing with fitness sensors embedded in the fabric<sup>6</sup>

<sup>2</sup> For a more complete treatment of these issues, see Scott Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 95 Texas Law Review 85 (Nov. 2014). See also Christopher Wolf, Jules Polonetsky, and Kelsey Finch, *A Practical Privacy Paradigm for Wearables* (Future of Privacy Forum, Jan. 8, 2015).

<sup>3</sup> Fitbit Blaze, <http://www.fitbit.com>; Garmin Forerunner, <http://www.garmin.com>.

<sup>4</sup> LifeBEAM, <http://www.life-beam.com>.

<sup>5</sup> Sensoria Fitness Socks, Sensoria Fitness, <http://store.sensoriafitness.com>.

Medical devices, such as:

- Health monitors that can track blood glucose levels,<sup>7</sup> temperature<sup>8</sup> and breathing patterns<sup>9</sup>
- A brassiere that can track slight variations in skin temperature for use in detecting breast cancer<sup>10</sup>
- Epidermal electronic patches worn as a bandage that can detect temperature, heart rate, brain activity, hydration levels, exposure to ultraviolet radiation, and even blood stream variations including glucose or potassium levels and kidney function<sup>11</sup>
- Ingestible and implantable sensor devices including “smart pills” that can monitor pH levels, temperature, and other internal bodily functions<sup>12</sup>
- Sensors worn between two teeth or mounted on dentures or braces to assess dental disease or unhealthy dental habits<sup>13</sup>

Workplace or employee monitoring devices, such as:

- Sensors worn around or on the lower back that can detect poor posture or risk of back injury<sup>14</sup>

---

<sup>6</sup> OmBra, <http://www.omsignal.com>; Ralph Lauren PoloTech Shirt, <http://www.ralphlauren.com>; Athos, <http://www.liveathos.com>.

<sup>7</sup> Joseph Walker, *Easier Blood-Sugar Monitoring for Diabetics*, Wall Street Journal (June 29, 2015).

<sup>8</sup> Peak, Basis, <https://www.mybasis.com>.

<sup>9</sup> Spire, <http://www.spire.io>.

<sup>10</sup> Cyrcadia Health, <http://cyrcadiahealth.com>.

<sup>11</sup> Biostamp, MC10, <http://www.mc10.com>; Sano, <http://www.sano.co>.

<sup>12</sup> Given Imaging, <http://givenimaging.com>.

<sup>13</sup> Ross Brooks, *Tooth-Embedded Sensor Relays Eating Habits to the Dentist*, PSFK (July 30, 2013).

<sup>14</sup> Lumo Back, Lumo, <http://www.lumoback.com>; Upright, <http://www.uprightpose.com>.

- Employee identification badges or lanyards that can record time spent at an employee's desk, tone of voice, and proximity to other employees to measure productivity and work habits<sup>15</sup>
- A wristband to track when workers lift heavy objects to provide safety analytics<sup>16</sup>

Cognition and emotion devices, such as:

- A bracelet to track changes in a user's autonomic nervous system to detect mental state (e.g., passive, excitable, pessimistic, anxious, balanced)<sup>17</sup>
- Headbands to track brain activity, focus and cognitive performance<sup>18</sup>
- An electronic mood ring that can track emotional well being<sup>19</sup>

This is by no means an exhaustive list, but it is suggestive. It illustrates both the incredible innovation in wearable devices and the intimate details such devices can sense, record, and transmit.

## **II. Four Risks: Lax Security, Misuse, Re-identification, and Lack of Consent**

These wearable devices share four risks to which industry and lawmakers should attend: lax security, context-violative data uses, re-identification, and lack of meaningful consent.

<sup>15</sup> Humanyze, <http://www.humanyze.com>.

<sup>16</sup> Kinetic, <http://www.wearkinetic.com>.

<sup>17</sup> W/Me Bracelet, <http://www.rootilabs.com>.

<sup>18</sup> Muse headband, <http://www.choosemuse.com>; Melon headband, <http://www.dagri.com>.

<sup>19</sup> Moodmetric, <http://www.moodmetric.com>.

1. Wearable Devices are Prone to Data Security Problems: Many wearables are small consumer devices such as a fitness-tracking bracelet, a health monitoring patch, or a smart watch. Recent news has highlighted that such devices often have inadequate data security protections. A February, 2016 report, for example, showed that of eight wearable fitness devices studied, only one—the Apple Watch—had properly secured the device's Bluetooth connectivity.<sup>20</sup> These problems are not new: researchers have been demonstrating such vulnerabilities for years.<sup>21</sup> They persist because wearables have limited form factors, which can make robust security more difficult to implement, and often relatively low target price points, which can make incorporation of security measures prohibitive. In addition, these devices are often developed by startups or other firms unfamiliar with or not focused upon data security issues. Finally, these devices often have limited processing power and limited Internet connectivity abilities, making it difficult to push software-based security updates to them to address discovered security flaws.

These data security vulnerabilities create various policy decisions for lawmakers. I will mention two. First, Congress should confirm that the Federal Trade Commission (FTC) has authority under Section 5 of the FTC Act to oversee data security, as was recently affirmed in the Wyndham case by the U.S. Court of Appeals for the Third Circuit.<sup>22</sup> Much has been written and said about this, so I will not dwell on it.

---

<sup>20</sup> Open Effect, Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security (Feb. 2, 2016).

<sup>21</sup> Mahmudur Rahman et al., *Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device* 1 (Apr. 20, 2013).

<sup>22</sup> FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).



Second, and more broadly, if Congress continues to consider Federal data breach notification legislation, it should ensure that such legislation protects wearable device data (and “Internet of Things” sensor data generally). The vast majority of state data breach notification laws do not protect the biometric and sensor data produced by wearable devices.<sup>23</sup> If consumers’ wearable device data were hacked from a device or from the cloud, at the moment most device manufacturers would be under no obligation to warn the public. Data breach notification statutes help the market to discipline firms with lax security by providing the public with the information it needs to make informed consumer choices. Wearable device data—particularly biometric data—should be included in these legal regimes. The states should include biometric sensor data created by wearable devices in their definition of what constitutes protected data, and/or Congress should do so if it adopts a Federal data breach notification statute.

2. Wearable Device Data Invite Misuse: A consumer knows that wearing an exercise monitor will create data that reveals her exercise habits or sleep patterns. These inferences are obvious and direct. Wearables permit far less obvious inferences, however, that consumers may not expect. As a simple example, research shows that seemingly innocuous accelerometer data—generally used to show how a person is moving in space—can be used to detect location because the movement pattern created by driving down a particular road is often unique and therefore identifiable.<sup>24</sup>

<sup>23</sup> See Peppet, *supra* note \_\_ at 139-140 for a full review of these state law issues.

<sup>24</sup> Jun Han et al., *ACComplice: Location Inference Using Accelerometers on Smartphones*, in 2012 Fourth International Conference on Communication Systems and Networks (COMSNETS 2012).

More generally, the data created by wearable device sensors are both massive in quantity—a sensor may track habits or behavior 24/7—and very high in quality. A wearable fitness monitor may track location, three-dimensional movement, heart rate, or other characteristics accurately, precisely, and persistently. This massive quantity and high quality of data can permit unexpected inferences. For example, a fitness monitor’s separate measurements of heart rate and respiration might in combination reveal not only a user’s exercise routine, but also cocaine, heroin, tobacco, and alcohol use, each of which produces unique biometric signatures.<sup>25</sup> As wearables proliferate, we are likely to find new and more startling inferences. For example, exercise data might permit inferences about a person’s character, motivation, employment habits, and even credit-worthiness (e.g., if a person exercises a lot, they are likely diligent and hard-working).

Consumers are rightly nervous about such unexpected uses of wearable device data. A preliminary study found, for example, that Americans are concerned about health-related data being used outside of the medical context: 77% worry about such data being used for marketing, 56% are concerned about employer access, and 53% worry about insurer access.<sup>26</sup> Industry and lawmakers should be clear that such wearable device data will not migrate into employment, credit, insurance, housing, or other decisions without meaningful notice to consumers.

In addition, consumers should not be pressured into disclosing such data. In other contexts we have seen state legislatures forbid insurance companies, for example, from

---

<sup>25</sup> Annamalai Natarajan et al., *Detecting Cocaine Use with Wearable Electrocardiogram Sensors*, in UbiComp’13: Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing 123, 123 (2013).

<sup>26</sup> Heather Patterson and Helen Nissenbaum, *Context-Dependent Expectations of Privacy in Self-Generated Mobile Health Data* 43-45 (June 6, 2013).

requiring access to vehicular “black box” data as a condition of automotive insurance.<sup>27</sup> Such use constraints allow consumers to adopt such new technologies without fear that their data will end up in the hands of an employer, insurer, bank, or landlord. To the extent that it considers taking action in the wearable device context, Congress should consider similar constraints on the migration of wearable device data.

Finally, consumers should be protected against “in house” migration of wearable device data from one type of use to another. The Fair Credit Reporting Act (FCRA), for example, applies to third-party consumer reports used in credit or employment decisions but does not cover analytics performed by an employer on data generated by employees wearing a fitness device or other wearable technology. As wearable devices proliferate in the workplace, employees are concerned that data ostensibly collected for one purpose—such as participation in a wellness program—might be used for another purpose—such as performance evaluation. Given the powerful inferences an employer might draw from an employee’s biometric or other data (e.g., fitness, smoking, or nutrition habits, etc.), new safeguards against such data migration should be considered.

3. Wearable Device Data Are Relatively Easy to Re-Identify: Much privacy law and regulation depends on anonymizing or de-identifying data sets to protect privacy.<sup>28</sup> Unfortunately, data produced by wearable device sensors are particularly difficult to de-

<sup>27</sup> Ark. Code Ann. § 23-112-107(e)(3)-(4); N.D. Cent. Code § 51-07-28(6) (2007); Or. Rev. Stat. § 105.932 (2013); Va. Code Ann. § 38.2-2212(C.1)(s) (2007).

<sup>28</sup> Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010).

identify reliably.<sup>29</sup> Recent research from MIT on location data streams, for example, shows that it is relatively easy to re-identify such information: researchers were able to pick out an individual mobile phone user from an anonymized data set of over 1.5 million such users using only four known data points (e.g., that the individual was at location X or Y at time A during the course of the year).<sup>30</sup> This is a remarkable result, and illustrative of the reality that wearable device data is prone to re-identification. The reason is simple: sensor data can capture such a rich picture of an individual that each individual in a sensor-based data set is reasonably unique and therefore identifiable. Heartbeat data, for example, has been shown to be a reliable, if unexpected, biometric identifier.<sup>31</sup>

This creates regulatory problems for all privacy regimes that depend on the assumption that data can be easily protected through anonymization. Specifically, easy re-identification challenges the distinction between legally protected "personally identifiable information" (PII) (e.g., name, address, social security number) and other data that the law affords lesser protection. If wearable device data sets are easily re-identifiable, then all data coming off of such devices may need to be considered personally identifiable. This ties to my suggestion above that if Congress takes up Federal data breach notification legislation, it should be careful to include biometric or other sensor-based data in its definition of PII. More broadly, Congress may need to expand the various definitions of PII found in Federal statutes to include the data created by wearable devices.

---

<sup>29</sup> Andrew Raij et al, *Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment*, in Chi 2011: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 11 (2011).

<sup>30</sup> Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, Sci. Rep., Mar. 25, 2013.

<sup>31</sup> Yogendra Narain Singh, *Individual Identification Using Linear Projection of Heartbeat Features*, Applied Comput. Intell. & Soft Comput. (2014).

4. Meaningful Consent is Currently Lacking: Wearable devices are generally small and often have no screen or other complex user interface. As a result, showing a user a privacy policy or other agreement on the device itself is often difficult or impossible. Such privacy notifications could be shipped with the device in the box or package, but currently manufacturers generally do not provide such information.<sup>32</sup> Instead, consumers are left to search out privacy information on a manufacturer's web site, where it is often difficult to locate, confusing, or not specifically focused on the privacy concerns created by wearables. In particular, existing privacy policies often fail in the following respects:

- They often fail to clarify whether biometric or other sensor data collected by a wearable device is considered "personally identifiable information" under the policy;
- They often do not clarify whether consumers own and can access, control, or delete sensor data created by their wearable devices, or they specify that the manufacturer and not the consumer has such rights;
- They often do not explain what data the device collects, what sensors it deploys, and where such data are stored (e.g., on the device, on a user's smartphone, in the cloud, or on the manufacturer's servers);
- They often do not clarify to what use the manufacturer expects to put the data, with whom it will share the data, or by what constraints on use the manufacturer will abide.

Regulators must continue to work with industry to strengthen and clarify such policies, encourage manufacturers to provide such policies in multiple locations and in

---

<sup>32</sup> See Peppet, *supra* note \_\_ at 142-43 (showing that none of twenty popular devices were shipped with privacy policy information in the packaging).

simple terms, and sanction firms with materially misleading policies. The Federal Trade Commission's January, 2015 report titled *Internet of Things: Privacy and Security in a Connected World* took steps in this direction. It also sought general Federal privacy legislation authorizing the Commission to mandate basic privacy protections, including privacy disclosures and consumer choice, even absent a showing of deception or unfairness.<sup>33</sup> Although the Commission did not seek legislation targeted directly at the Internet of Things or wearable devices particularly, it noted that generalized Federal privacy legislation would make it possible for the Commission to strengthen notice to consumers about the privacy implications of these new devices. Such legislation would be well advised to protect consumers and ensure that they continue to adopt and deploy wearable devices in their many forms.

---

<sup>33</sup> Federal Trade Commission, *Internet of Things: Privacy and Security in a Connected World* viii (Jan. 2015).

Mr. BURGESS. The Chair thanks the gentleman. Mr. Webster is recognized for 5 minutes for your testimony, please.

#### STATEMENT OF DOUG WEBSTER

Mr. WEBSTER. Thank you, Mr. Chairman and members of subcommittee. The Internet has revolutionized the world around us, transforming the way we use and share data to communicate, to collaborate, and consume entertainment and information. Yet, the next wave of technology isn't about moving data from one place to another, it is about connecting physical objects to the Internet on an unprecedented scale.

Now, increasingly, the things connected are the shirts on our backs, the glasses on our foreheads, the watches on our wrists, and the jewelry around our necks, and collectively, these emerging devices are referred to as wearables.

To be sure, some wearables are mere novelties. However, many others, like the Fitbit or Apple watch, are improving our health and wellness by tracking our daily activities, and the most advanced wearables have the power to save lives and improve patient outcomes. For example, there is an FDA-approved heart rate monitor that provides precise information from cardiac patients to their physicians between visits to the doctor's office.

Another device looks like a typical smartwatch, but in reality, it helps epileptic patients manage their stress and alert family members and physicians when a convulsive seizure happens.

And a third, a prototype in development, is a glucose-monitoring contact lens that allows diabetics to monitor their blood sugar continuously, and the possibilities are endless here. I mean, virtual reality goggles that provide for immersive education, connected football helmets to alert the team physical to a possible concussion, GPS-enabled slippers to make sure an elderly relative is getting out of bed and doesn't wander off, and accessories that make mobile payments faster and easier.

Now, the one feature that unites these devices is their wireless connectivity to the Internet. Each contains a tiny radio transmitter that sends data to a receiving device, such as a WiFi router or a smartphone, and then the data is transmitted over an IP network to a server or data storage facility.

Now, once online, software allows you to visualize and analyze the data to help improve decisionmaking, whether it is information about your daily run, your average number of steps per day that gauge your fitness progress, or simply storing videos so you can decide whether to post it at a later date.

Now, at Cisco, we have been monitoring the growth of wearables for 3 years, and it is fair to say that these devices are poised to take off. Here is the forecast from our most recent Cisco mobile visual and networking index report. By 2020, we forecast approximately 600 million wearable devices globally, up from 97 million in 2015.

Now, fewer than 15 percent of these devices are expected to be directly capable of transmitting on a cellular network. Most, instead, will use WiFi or Bluetooth to connect to the Internet. Now, the data generated by wearables represents a tiny trickle in the

larger stream of mobile data, mostly because only a few of these devices are being used to transmit video.

Traffic from wearables is forecast to account for only 1 percent of total mobile data traffic by 2020, even as the amount of data generated by each device is expected to grow.

Now, North America has a 40 percent share of global connections today, and it is because we are early adopters, but that falls to 30 percent by 2020 as Europe and Asia catch up with us. By 2020, there are forecasts to be over 180 million wearable devices in use in North America, compared to about 40 million today, representing a 4 1/2-fold increase in just 5 years.

Now, given this growth, it is important for policymakers to understand the issues affecting wearables. We need to ensure that radio spectrum is available with the right set of rules to make sure these devices can connect to the network, to encourage policy that support investment in the service provider networks that are needed to transport data to the Internet.

We need policies that encourage startups and small companies by ensuring access to venture capital to tax policies that support research and development, as well as encouraging more young people to enter careers in science, technology, engineering, and math, also known as STEM. And we need to ensure that device manufacturers and applications developers understand privacy and security threats and take the steps to protect their devices and the personal information of consumers.

Here is the bottom line: Wearables represent a measurable component of the mobile landscape, and they are projected to continue to grow. They hold incredible promise to improve our lives. Public policies that encourage the development of this category should be supported so that the United States can continue to be a leader in this next chapter of the Internet.

Thank you for your attention, and I look forward to answering your questions.

[The statement of Mr. Webster follows:]



**Doug Webster, Vice President, Service Provider Marketing, Cisco**  
**Subcommittee on Commerce, Manufacturing, and Trade**  
**Hearing: "Disrupter Series: Wearable Devices"**  
**Thursday, March 3, 2016, 10am**

Thank you Mr. Chairman and Members of the Subcommittee:

The Internet has revolutionized the world around us – transforming the way that we use and share data to communicate, collaborate and consume entertainment and information.

Yet, the new wave of transformation isn't just about moving data from one place to another. Today, the challenge is connecting physical objects to the Internet, on an unprecedented scale.

Increasingly, the "things" being connected are the shirts on our backs, the glasses on our foreheads, the watches on our wrists, and the jewelry around our necks. Collectively, these emerging devices are referred to as "wearables."

To be sure, some wearables are mere novelties, such as the selfie hat.

However, many others - like the Fitbit or Apple Watch – can actually help improve our health and wellness by tracking our daily activities. And the most advanced, purpose-built wearables can save lives and improve patient outcomes.

- For instance, there's an FDA approved heart rate monitor that provides precise information from cardiac patients to their physicians between visits to the doctor's office.
- Another device looks like a typical smartwatch. But in reality it helps epileptic patients manage their stress and alert family members and physicians when a convulsive seizure happens.
- A third, a prototype in development, is a glucose-monitoring contact lens that allows diabetics to monitor their blood sugar continuously.

The possibilities are endless, and limited only by our imaginations.

There are virtual reality goggles, connected yoga pants, bracelets that help you fight food cravings, and rings that you can use for mobile payments. And that's just the tip of the iceberg.

The one feature that unites these devices is their wireless connectivity to the Internet. Each of these devices contains a tiny radio transmitter that sends data to a receiving device – such as a Wi-Fi router or smartphone. Then, the data is transmitted over an IP network to a server or data storage facility.

Once online, software allows you to visualize and analyze the data to help improve decision-making – whether it's information about your daily run, your average number of steps per day, health metrics, or even simply storing video so you can later decide whether to post it on YouTube or Facebook.

At Cisco, we've been monitoring the growth of wearables for three years, and it's fair to say that these devices are poised to accelerate with consumers, health care providers, and even on the assembly line. Here's the forecast from our most recent mobile visual network index report.

- Cisco forecasts that there will be 601 million wearable devices globally by 2020, up from 97 million in 2015, a compound annual growth rate of 44 percent.
- By 2020, fewer than 15 percent of those devices will be directly capable of transmitting on a cellular network – most will use technologies such as Wi-Fi or Bluetooth to connect to the Internet.
- The data generated by this category of devices represents a tiny trickle in the larger bucket of mobile data, mainly because few of these devices are being used to transmit video. Traffic from wearables will account for about 1 percent of total mobile data traffic by 2020, even as the amount of data generated by each device is expected to grow.
- North America has a 40 percent share of global connections today – we are early adopters. But that falls to 30 percent by 2020 as European and Asian consumers catch up with us. By 2020, there will be over 180 million wearable devices in use in North America, compared to around 40 million today.

Given this growth, it's important for policymakers to understand that the issues affecting wearables are significant.

- We need to ensure that radio spectrum is available with the right set of rules to make sure these devices can transmit.
- We need to encourage policies that support investment in the wireless networks and wired networks needed to transport data to the Internet.

- We need policies that encourage start ups and small companies by ensuring access to venture capital, pro-growth tax policies that support research & development, as well as encouraging more young people to enter careers in the STEM fields.
- And we need to ensure that device manufacturers understand the privacy and security threats, and take proactive steps to protect their devices and the personal information of consumers.

Today, wearables represent a measurable component of the mobile landscape and they are projected to have a significant growth trajectory. They also hold incredible promise to improve our lives. Public policies that encourage the development of the category should be supported so that the U.S. can continue to be a leader in this next chapter of the Internet.

Thank you for your attention, and I look forward to answering your questions.

Mr. BURGESS. The Chair thanks the gentleman. Thanks to all of our witnesses for your testimony. We will move into the question-and-answer portion of the hearing.

I would begin the questioning this morning by recognizing Mrs. Brooks from Indiana for 5 minutes for questions.

Mrs. BROOKS. Thank you, Mr. Chairman. Thanks for holding this hearing. I happen to be one of those brand new users, just acquired a couple of weeks ago. I kind of wish I had been a part of this hearing before I bought this. However, I am excited to be part of the wearable technology consumer base, and, in fact, bought several of these for my parents and in-laws for the holidays.

And so we often think about fitness trackers when we hear wearable technology, and so we are certainly learning a lot, and when, in preparing for this hearing, learning about innovations in manufacturing. In Indiana where I am from, is a heavy manufacturing State, one of the top manufacturing States in the country.

And so, Mr. Bianculli—I am not sure I caught—

Mr. BIANCULLI. Bianculli, yes.

Mrs. BROOKS [continuing]. Bianculli, what kind of cost savings—can you talk a little bit more about wearables with respect to manufacturing?

Mr. BIANCULLI. Sure.

Mrs. BROOKS. What kind of cost savings can be expected in this area, and how do we achieve this in the manufacturing sector?

Mr. BIANCULLI. Yes. Absolutely. Thank you, Congressman.

Looking in the manufacturing sector and breaking it down really into kind of three major components: raw materials coming into a manufacturing facility, those raw materials being processed in the outbound side of that where the goods are sorted, picked, packed, loaded, and then transported down the supply chain. Some of the early adoption we are seeing for the kinds of wearables I spoke about, which is basically being able to capture and get the right information in front of a worker in real time have been on the third category, picking, packing, sorting.

Think about an eCommerce order that is being built, think about an order that is coming from a manufacturer to a distribution center, being able to sort the goods, load those goods, be able to optimize the volumetric efficiency of those goods onto a trailer or onto a pallet for distribution. A lot of these cases, we are starting to see be adopted or using wearables to seamlessly present information in front of the user as they are going through their workflow to be able to get the right goods in the right place, to be able to optimize the way they are loaded onto vehicles, and to be able to get them down and through the supply chain faster than they have previously.

So it is really about worker productivity. I use the word in my testimony about frictionless workflow, so think about it as taking the—literally taking the friction out of the workflow and allowing workers to simply get their job done and let the technology take a back seat and just augment their capabilities.

Mrs. BROOKS. Thank you. Ms. Burich. So my daughter was a college athlete and—but many—several years ago, and so none of this technology. In fact, when she was in youth soccer, that is when Under Armour came to be, OK. So just talking about that type of

advancement during this time period and now all of this wearable technology. What do you anticipate—how do you anticipate it being used from the youth—the youth sector all the way up to the professional athlete sector?

Ms. BURICH. Yes. We look at the market in terms of like team sports and individual sports or individual—

Mrs. BROOKS. Can you turn your mike on, please.

Ms. BURICH. We look at the market in terms of like team sports, organized sports, which is what you are referring to, and then individual use for fitness, so where we have our elite system, it is very sophisticated, and there is definitely an opportunity to translate it for youth sports, and I would say recreational team sports to high school, even colleges who can't afford the solution today. So that is a development and an opportunity for growth, and again, it is something that the technology and capability is there and it should be accessible to more—to broader population.

And then, I think, just connecting that down, there is probably—it turns into more of the individual use case where you want kids in phys ed to be using technology so that it is—they are not—so that you are giving them the right amount of exercise for their fitness condition, and you are not overstressing them.

Mrs. BROOKS. And these kids at all ages are so tech savvy from a very, very young age—

Ms. BURICH. They like it.

Mrs. BROOKS. —so they are going to love this.

Mr. Webster, just shifting gears very briefly, you talked about the spectrum. Are most wearable devices operating on unlicensed spectrum or licensed spectrum, if you know, and could the spectrum be an obstacle hindering widespread adoption of these devices? We are getting ready to have an auction with respect to the spectrum. Can you just talk a little bit more about the spectrum issues?

Mr. WEBSTER. Yes, ma'am. Our forecast indicates about 15 percent of all wearables will directly be connected to the Internet that would be using a license spectrum. The vast majority or 85 percent of them will be connected via unlicensed spectrum to the respective Internet-connected device.

Now, it is important to know that wearables is just one small part of an even larger Internet of Things—

Mrs. BROOKS. Right.

Mr. WEBSTER [continuing]. Initiative, and so when you take that all en masse, then absolutely, the importance of continuing to increase the amount of license and unlicensed spectrum will be key to help really make this industry segment that is so beneficial to so many continue to prosper.

Mrs. BROOKS. Thank you. Thank you all for your testimony. I yield back.

Mr. BURGESS. The gentlelady yields back. The Chair thanks the gentlelady. The Chair recognizes the gentlelady from Illinois, 5 minutes for questions, please.

Ms. SCHAKOWSKY. Mr. Peppet, I am going to ask you some questions, but I wanted to first—this idea of kids. To me, I am a little concerned about that. Is this going to be more anxiety-provoking,

now we are measuring and another way that you have to look at an electronic device.

I am just wondering if Adidas, in marketing to children, has talked to child psychologists, to educators on whether or not, as you say, that forget the awkward, social situation, et cetera, I mean, that could be a positive. But I feel like now encouraging kids to measure their every step or their heart rate or something, I am just wondering if you have done the kind of research I think would be important before we really market this to grammar school kids, or middle school kids.

Ms. BURICH. I would say in that space, we are providing a piece of a system that our partners are providing them to the schools. I don't know how much research they have done in that area. I know they have done research and they have positive findings from the use of technology related to attendance and kids' grades and other things that this is impacting.

Ms. SCHAKOWSKY. There is also, you know, a real pushback on all the testing that is going on. I kind of feel like this may be in that category. I just wanted to raise that. I don't immediately accept that this is a great thing to push to kids.

But anyway, let me just raise that and go on to Mr. Peppet, who actually—and you have a quote at the beginning of your testimony: Very soon we will see inside ourselves like never before with wearable, even internal sensors that monitor even our most intimate biological processes. It is likely to happen even before we figure out the etiquette and laws around sharing this knowledge.

In a way, I think I am getting at that with that earlier question, but here is what I want to get more specific.

In January of last year, the Federal Trade Commission released a report entitled "Internet of Things: Privacy and Security in a Connected World." In the report, the FTC states that there is, quote, a "need for substantive data security and breach notification legislation at the Federal level" and that such legislation should, quote, "protect against unauthorized access to both personal information and device functionality."

So in your testimony, Professor Peppet, you say that small sensor-based connected devices like wearables are inherently prone to security problems. Can you explain what you mean by that? What are some of the vulnerabilities specific to wearable devices?

Mr. PEPPET. Sure. Thank you for the question. As I said, the devices tend to be small, they tend to be designed for a low price point, and they tend to have very limited computing and even communication power, and that presents a whole set of security challenges.

When the first wave of fitness trackers came out, computer science, you know, security folks discovered very quickly how easy it was to hack into them, largely because they hadn't secured whether it was the Bluetooth connectivity or the WiFi connectivity, whatever they were using, they hadn't secured those connections. And you know, that was several years ago, some of those studies were done.

A study came out, I think, three weeks ago, testing some of the most current and most popular versions of those devices and found, essentially, the same set of results. So when I talk with computer

scientists, this is a real technical problem because they are small, and it is very hard to design security in a comprehensive way.

It will happen, but the FTC, for example, has really been pushing companies to try harder.

Ms. SCHAKOWSKY. So would you say the biggest barrier is that there are technical issues, or are these wearable manufacturers taking into account security sufficiently, or even thinking about it?

Mr. PEPPET. I think it is both. Excuse me. I think it is both on the technical side, as I already described. On the are-they-trying-hard-enough side, there is at least two problems. One is a lot of these devices originally have been coming up as start-ups, and start-ups often, you know, are rushing to market with a product, may not spend enough time on data security.

The converse problem is interesting, too, which is some of these devices have come out of very big companies, very established companies that don't have much experience with the data stack. They are not IT companies. They are some other sort of firm, and so when they venture into the tech space—and we have seen examples of this—they may not have the either expertise or the depth to build that kind of security.

Ms. SCHAKOWSKY. Well, let me ask you this: Get to the regulatory part. You pointed out Texas. I actually have a bill, too, that would require breaches to be—also this biometric stuff and to be—consumers to be reported. Should we follow Texas' lead in requiring that notification as well?

Mr. PEPPET. I think we should. Whether States do it or Congress does it, I think that consumers should know if their biometric data or other sensor-based biologic data has been hacked. I think you would choose between fitness—you know, the two of you each had fitness devices. I think you might choose which one you wanted if you knew that one of them, the data had been stolen. So yes, I think that is something that we should do for consumer—

Ms. SCHAKOWSKY. I am going to submit the rest of my questions for the record, and I really appreciate all of you. Thank you. I yield back.

Mr. BURGESS. The gentlelady yields back. The Chair thanks the gentlelady. The Chair recognizes the gentleman from New Jersey, Mr. Lance, 5 minutes for questions.

Mr. LANCE. Thank you. Mr. Webster, we have heard a lot about the benefits of this technology. Why is it more advanced, for example, than the smartphone?

Mr. WEBSTER. Well, Congressman, I believe that it is one part of the broader ecosystem. The sensors can be in a number of different places and across all different industry verticals and aspects of our lives. Oftentimes, they will pair it with a smartphone or another Internet-connected device, and then that data then will go back to a cloud area or data center where analytics can be done. So while, oftentimes, the focus on these types of discussion is on the sensor itself, the reality is it is the full ecosystem and how they are all interrelated.

And that is why we believe, at Cisco, it is very important that there is security by design and privacy by design in each and every one of those parts so that you are able to look at it in aggregate

as opposed to just looking down on one aspect of the broader ecosystem.

Mr. LANCE. Thank you. My son got a—would it be called a smartwatch?—for Christmas. I don't have one yet, but I am sure he will inform me about all of this as he does on so much of the technology, and thank you for the testimony of the entire panel. It is certainly the wave of the future, and I am pleased that the chairman and the ranking member have chosen to hold this hearing, and I yield back the balance of my time.

Mr. BURGESS. The Chair thanks the gentleman. The Chair would note that there are votes on. Mr. Harper, I will recognize you for 5 minutes for questions, but I do want to point out to you the Chair has not taken his time for questions yet, so govern yourself accordingly.

Mr. HARPER. With that, I will be brief and respect my chairman.

Thank you all for being here. Mr. Webster, if I could ask what types of economic and workplace problems do wearables solve for business?

Mr. WEBSTER. Congressman, wearables can solve a number of different problems. We discussed a little bit about the medical benefits that could be coming about and how it pertains to workers in hospitals. There is a great example about assembly line workers that were going through, and because they have wearables that are giving them step-by-step instructions when they are doing their quality checks, there is measurably less defects, and a much greater quality of the products that are served, and especially as you start going into more complex maintenance areas, especially safe for remote workers. They are going to be able to go and create a much higher quality of step-by-step instructions,

Mr. HARPER. Mr. Bianculli, can you comment on that as well?

Mr. BIANCULLI. Certainly. Yes, we are seeing a host of opportunities. Something I would call—the movement in the consumer space has really been around Fitbit and these other—Adidas as well—around something called quantified self. So quantifying my behaviors, and what we are seeing in the enterprise markets is quantifying environments, quantifying workflow, you fundamentally can't improve what you can't measure. And so the use cases we are seeing are capturing those trapped inefficiencies that are there because we are not able to quantify what is happening in a given workflow, and basically, you could think about it as, you know, in a large tier 1 transportation company who might employ, or large retailer who might employ 300,000 people to restock shelves every evening in a retail store, understanding the workflow of each one of those 300,000 workers, which ones are performing in the best ways possible, and then helping the others to be able to achieve that level of performance by quantifying the environment.

Mr. HARPER. All right. Thank you very much.

Mr. BIANCULLI. So lots of opportunities around quantifying the workflow.

Mr. HARPER. Thank you. Mr. Palliparambil, given NXP's presence in many of the wearable devices on the market today, do we currently have the infrastructure to support the rapidly growing wearables market and accommodate multiple users?



Mr. PALLIPARAMBIL. Yes, sir. Thank you for the question. Yes, we do, and as you pointed out, the Adidas products and some of the products from Zebra, so we have the sensors, we have the micro controllers and the security element that I talked about in my testimony, which allows to provide that level of security and often preferences for the consumer is available today. The technology is available. It is just a matter of choosing to use it.

Mr. HARPER. Thank you.

Mr. PALLIPARAMBIL. Thank you.

Mr. HARPER. In the interest of time, I am going to yield back. The chairman may want to talk. Thank you.

Mr. BURGESS. The Chair thanks the chairman. We have been joined by Mr. Bilirakis of Florida. Mr. Bilirakis, I will recognize you for questions. You know we have votes on. The Chair has generously allowed members to go before the chairman's time, so do bear in mind both you and I have to ask questions.

Mr. BILIRAKIS. OK.

Mr. BURGESS. I will recognize you for 5 minutes and hope that you don't—

Mr. BILIRAKIS. Well, I will yield.

Mr. BURGESS. I hope that you don't use all of it.

Mr. BILIRAKIS. I yield to the chairman.

Mr. BURGESS. No, no. I want you to go ahead.

Mr. BILIRAKIS. OK. All right. I won't use all of it, promise you.

For the whole panel, what are the incentives for business and consumers who are not using wearables to start utilizing wearables and this kind of technology now? And this is for the whole panel.

Ms. BURICH. I can take it.

Incentive. I think there is a lot of data that shows that when you use a wearable, it can really help you stay on your fitness journey longer. I mean, there is also data that shows the more active and fit you are, it prevents disease, it keeps you out of the healthcare system. So it is a proactive way to manage your health.

Mr. BILIRAKIS. Very good.

Anyone else.

Mr. PALLIPARAMBIL. Sure. So for a regular consumer, beyond fitness tracking and health, using a wearable for multiple applications, like payments, transit, and access into buildings, so logical and physical access. So the same wearable can, today's technology, allows you to use it for multiple applications, so beyond life and fitness. And that is the big advantage that I see, where you can have frictionless movement. So you have convenience, but you have the security to conveniently use this in your everyday life.

Mr. BILIRAKIS. Thank you.

Anyone else.

Mr. WEBSTER. Congressman, the benefits of wearables that I have seen, in general, really it comes down to a competitive issue. It is allowing people to be more productive, businesses to gain more productivity. It is going to help empower those that are using this is a way that can't be matched in other ways.

So it is very much a competitive issue, and I think it is very important that policymakers take the steps to really help propel this industry forward with the appropriate safeguards that we can maintain appropriate competitive positioning.

Mr. BILIRAKIS. Very good. Thank you.

Anyone else?

Mr. BIANCULLI. Congressman.

Mr. BILIRAKIS. Yes, please.

Mr. BIANCULLI. Congressman Bilirakis, I would say we break this down to two components. One is the input side of wearables, so being able to collect information about a particular workflow or what is happening in a given environment. So that is the input side. Think of that as Internet of Things sensor connectivity.

And then the wearable instructive part of this, which is being able to aim somebody in the right direction, being able to give them information on their wrist or a heads-up presentation of information while they are going through a workflow.

So think about the input side as being the Internet of Things of wearables, and think about the output side as being an efficient mechanism for being able to consume the data that is generated by the Internet of Things sensing technology.

Mr. BILIRAKIS. Very good. Thank you.

Anyone else?

Mr. PEPPET. And then just very briefly, another incentive is that consumers in some contexts are being paid to use these devices. So many consumers, for example, myself, my healthcare plan at my employer gives me discounts if I use a wearable and track my fitness. We have also seen a life insurance company that has now issued a life insurance policy that gives you a discount on your premiums if you track your fitness using a wearable. So there are all sorts of actual direct incentives being used as well.

Mr. BILIRAKIS. Very good. Thank you.

And I will yield back, Mr. Chairman. Thanks for the opportunity.

Mr. BURGESS. The gentleman yields back. The Chair thanks the gentleman.

I will now recognize myself for questions.

And I do, again, want to thank you. This has been a fascinating hearing. Again, we do have a vote on, but let me see what I can get through.

Mr. Peppet, you brought up something that actually I am very interested in.

And, Mr. Webster, obviously, some of the work you do in the healthcare space. The Affordable Care Act has brought us insurance with deductibles unlike anything anyone has ever seen.

But I guess what I am interested in is your comments, Mr. Peppet, on the monetization of the wearable or the monetization of the data and the ability to, perhaps, forgive a portion of the deductible to get the patient's buy-in to the continuation of the monitoring. So unlike Ms. Burich's population, people won't drop out of the monitoring, they will continue because they are getting something positive.

Could either of you speak to that?

Mr. PEPPET. That is a very interesting question, and it is a very interesting domain, because you are exactly right that ongoing compliance with whatever the medical prescription is difficult for doctors to get patients to follow through. And both wearables and other Internet of Things devices, there is a smart pill bottle that

every time you unscrew the cap, it is connected to WiFi and sends a message to your doctor saying: They took their pills today.

Those sorts of devices do allow a medical facility, whatever it is, to extend their reach out to their patients in all sorts of environments, and that is a potential huge benefit.

Now, in terms of, I think your question precisely was about payment or how premiums—

Mr. BURGESS. To actually monetize the participation in the use of a wearable.

Mr. PEPPET. Yes, I am not sure I know enough yet to know how that is going to play out.

Mr. BURGESS. But you are experiencing it as a consumer in your insurance policy. Is that correct?

Mr. PEPPET. Yes, you are seeing it in the insurance space, that is right. And I think what we are seeing is a huge number of consumers are being introduced to wearables for the first time in those wellness programs, through that insurance vehicle.

Now, again, I am actually relatively in favor of that kind of incentive. The one concern I would express is, for example, in my own experience with the program that I am involved with, it was very hard to figure out or to get information about the use that the data would be put to. So when an employee or a consumer signs up for that kind of incentive, you want to make sure they know what they are signing up for.

Mr. BURGESS. Mr. Webster, just in general, is there a way to quantify the benefit from the use of some of these wearables in the healthcare space?

Mr. WEBSTER. Congressman, I don't claim to be an expert into the healthcare industry, but, no question, it is a major vertical where IoT is being leveraged. I think if we start looking at the quality of care that is able to be delivered, to the extent of the medical reach, as was mentioned, and also just, I think, to the well-being, knowing that an elderly relative is active, for example, or being able to track them down should they wander off, say, an Alzheimer's patient, I think there are a lot of benefits there that I think could be challenging to quantify from a monetary benefit, but all recognize that it is good from a social benefit as well.

Mr. BURGESS. Thank you.

Mr. Bianculli and Ms. Burich, you both have stuff that you brought with you. Would you spend just a minute and tell us what you have brought?

Let's start you, Mr. Bianculli.

Mr. BIANCULLI. Yes, certainly. We had mentioned in the testimony that we developed wearable categories in the early 1990s actually, particularly for warehouse workers. And that has evolved over the last 25 years. And so one of the capabilities we have today is a wrist-mount mobile computer that is worn on the wrist of a user inside of a warehouse or a distribution center-type facility; a ring scanner that is able to image, take images, and also read machine-readable codes, like bar codes, inside of a warehouse-type environment.

And so a user as they are, for instance, loading a vehicle with goods that are coming from, say, an e-commerce order online, they are scanning those packages with that scanner that is mounted to

their hand, loading them into the vehicle. Their hands are staying free—again, back to the frictionless notion before—allowing them to get their work done without having the technology get in the way.

And so this is a probably very early example of application of wearable inside the enterprise space. We have got the Bluetooth ring scanner connected to a mobile computer on the wrist. That mobile computer on the wrist is connected over a WiFi network back to the IT systems of some of these major carriers.

The second example, and a more recent one, and one that we continue to invest in and we are going to see more of over the next 3 to 5 years, is this notion of eye-level information. So being able to have a device, as I am showing here, be worn on the head and then present through a screen which, if you look at the screen just a couple inches from your eye, it is going to look like a 15-inch laptop screen floating right in front of you.

So if you think about working on an aircraft, where you may have several hundred thousand pages of schematic drawings about that aircraft, being able to bring up just the right drawing at the right moment that tells me what procedure I should do. Similarly, in battlefield and Government applications, where you might be working on a tank or a piece of heavy machinery out in the field, not having to deal with multiple devices, laptops competing with the sun and everything else that can get in the way, simply be able to pull that information up on the screen; or be able to, via the camera that is mounted on this, send the video that I am seeing, the particular piece of apparatus that I am looking at, back to a remote expert who can then talk me through a scenario for repair.

Thank you.

Mr. BURGESS. Thank you. And thanks for bringing the peripherals today.

Ms. BURICH, can you do the same with your—

Ms. BURICH. Yes, sure. And I think our coaches could wear that while their players are wearing this.

Mr. BURGESS. There you go.

Ms. BURICH. This the Elite jersey that professional athletes wear on the field that contains some sophisticated sensors in this pod that goes in the back of a shirt. And then there is integrated heart rate sensing.

So in terms of compliance, it is important to put it all into one wearable that they can put on and not worry about, that goes through consumer laundry or laundry without any special care. So that is the Elite.

Mr. BURGESS. Wait, wait, wait. You can put that through the laundry?

Ms. BURICH. Without this.

Mr. BURGESS. Oh, without that. OK.

Ms. BURICH. You can put this through the laundry.

Mr. BURGESS. Just in case anyone was wondering, we do have a vote on. And I have a voting card that I will go put in. I have actually laundered it twice and it seems to still work. So maybe you can work on that same kind of technology.

Ms. BURICH. Yes. And then these are some of our hardware devices for the consumer market, a high-end running watch and kind

of a mainstream fitness device that also has step counting on there. And I think that is the critical thing, is that throughout the day you need to be getting intensity, frequency, and volume in terms of your exercise. So we are learning that it is not just about your workout, it is about what you are doing all day.

And then these garments are the translation of the Elite for consumers. So you can, again, just snap in a heart rate monitor. It is directly reading your heart rate off your chest. These are FDA approved in terms of the sensors, so wearable for consumer population as well.

Mr. BURGESS. Very good. Well, thank you. Thank you for that.

I will tell you this was a fascinating hearing. And I apologize that we have had votes that have kind of disrupted things. This is a disrupter series, after all. But there is a lot that has been shared today.

One of the things that we hear a lot about is on the issue of encryption. We are hearing questions about privacy and security of data. Encryption seems to be one of those ways. But there also seems to be some problems with encryption.

So I am actually going to ask each of you to respond, I realize we are really out of time and I have to go vote, but I would like a response to or at least your thoughts on that. As we develop our policies going forward, how do you balance this privacy question? Is encryption the way to go?

And then, as we know, we have got the FBI concerned about the makers' ability to encrypt and whether or not that is a good thing from a law enforcement standpoint.

So that is one of the questions that actually may end up before this very subcommittee when it comes down to a legislative product.

But I can't thank you all enough for being here. Wait a minute, I have got to do this. Seeing that there are no further members wishing to ask questions or for any other purpose, I would like to thank all of our witnesses for being here.

Before we conclude, I would like to submit the following documents for the record by unanimous consent: a letter from the Competitive Carriers Association, a letter from the Mercatus Center at George Mason University. Without objection, so ordered.

[The information appears at the conclusion of the hearing.]

Mr. BURGESS. And pursuant to committee rules, I remind members they have 10 business days to submit additional questions for the record, and I ask the witnesses to submit their responses within 10 business days upon receipt of the questions.

So without objection, and thanking everyone once again, the subcommittee is adjourned.

[Whereupon, at 11:40a.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]



Competitive Carriers Association  
Rural • Regional • Nationwide\*

March 3, 2016

The Honorable Michael Burgess  
Chairman  
Subcommittee on Commerce, Manufacturing,  
and Technology  
House Committee on Energy and Commerce  
2125 Rayburn House Office Building  
Washington, DC, 20515

The Honorable Janice Schakowsky  
Ranking Member  
Subcommittee on Commerce, Manufacturing,  
and Technology  
House Committee on Energy and Commerce  
2125 Rayburn House Office Building  
Washington, DC 20515

Dear Chairman Burgess and Ranking Member Schakowsky:

Competitive Carriers Association (CCA) respectfully submits this letter for the record regarding today's hearing on "Disrupter Series: Wearable Devices." CCA is the nation's leading association for competitive wireless providers and stakeholders across the United States. CCA's membership includes nearly 100 competitive wireless providers ranging from small, rural carriers serving fewer than 5,000 customers to regional and national providers serving millions of customers. CCA also represents close to 200 associate members including vendors and suppliers that provide products and services throughout the mobile communications supply chain. From our members' experience constructing networks and providing wireless connections that help to facilitate continued innovation and growth in wearables, we have seen firsthand how new technology supports advances in healthcare, public safety, and economic opportunities. Importantly, these advances are not limited to densely-populated urban areas, but are changing lives in rural America as well.

In the rural Mississippi Delta, the University of Mississippi Medical Center, GE Care Innovation, and C Spire all collaborated to deploy and utilize wireless glucometers, sphygmomanometers (blood pressure cuffs), scales, and tablets that transmit vital health data and video conference to and from healthcare providers when necessary, which is helping to produce immediate results to control diabetes and reduce patient trips and admissions to the hospital. Similarly, in agricultural communities, connected devices, smartphones, and tablets are revolutionizing precision agriculture, with farms using 30 to 40 gigabytes of data per month during peak usage. On dairy farms, connected ear tags for cattle are monitoring and wirelessly transferring temperature and vital signs, animal tracking, and other characteristics that are improving the efficiency of the dairy industry. And in education, technology supporting distance learning is providing opportunities for students to learn beyond rural classrooms. These new innovations and opportunities only will continue to grow and expand, in addition to the constantly evolving wearable technology covering health, education, fitness, and other activities that consumers are utilizing across the nation.

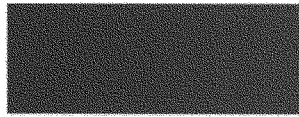
To foster continued growth, we appreciate policymakers' focus on promoting expansion of wireless broadband networks and help to ensure competition. This includes policies that make additional licensed and unlicensed spectrum available to help satisfy continued demand for mobile data in ways that provide carriers of all sizes meaningful opportunities to gain access to spectrum, as well as streamlining barriers to deployment of physical network infrastructure and ensuring access to backhaul

and networks. Congress should also ensure that existing and future support of the Universal Service Fund is focused on deploying broadband efficiently and effectively, including mobile broadband services. Wearables and other devices should be interoperable to the extent possible, so that consumers do not have to choose between access to the networks and systems that suit them best and the latest technology. Finally, policymakers should carefully consider privacy and security concerns to adequately protect consumers without placing undue burdens on carriers or other developers.

Wearables must continue to represent exponential growth in both urban and rural areas as progress continues towards 5G and the Internet of Things (IoT). If proper policies exist, wearable technology, like other IoT technology, can have a meaningful impact on underserved communities. CCA appreciates the Subcommittee's focus on this issue, and looks forward to continued work with policymakers to expand competition and innovation moving forward.

Please do not hesitate to contact me with any concerns.

Sincerely,



Steven K. Berry  
President & CEO  
Competitive Carriers Association



Statement for the Record

Adam Thierer  
Senior Research Fellow, Technology Policy Program  
Mercatus Center at George Mason University

March 3, 2016

House Energy and Commerce Committee  
Subcommittee on Commerce, Manufacturing, and Trade  
Hearing: "Disrupter Series: Wearable Devices"

Mr. Chairman and members of the Committee, thank you for this opportunity to submit a statement for the record on wearable devices. My name is Adam Thierer, and I am a senior research fellow at the Mercatus Center at George Mason University, where I study technology policy.

My statement will address how wearable technologies will impact economic growth, how policymakers should approach wearable technologies, and how cybersecurity and privacy concerns should be addressed. Wearable technologies, or "wearables," are a significant subset of my broader research on the "Internet of Things" or "IoT." Appended to this statement are two documents. The first is a compendium of reports on the economic impact of the IoT and wearables that I coauthored with Andrea Castillo, and the second is a *Reason* article, "Uncle Sam Wants My FitBit," further summarizing my perspective on the regulation and economic impact of wearables.

The projected number of Internet-connected devices, including wearables, is projected to grow by an amount anywhere from 19 billion devices to 40 billion devices by 2019. The global productivity gains from connected devices, including wearables, is expected to be between \$2.3 trillion and \$11.6 trillion over the next decade. In the healthcare sector alone, of which wearables perhaps most directly apply, the cost savings and productivity gains are calculated to be between \$1.1 trillion and \$2.5 trillion by 2025.

The topic of today's hearing is important in broader policy discussions about the IoT because wearables, as we write in our appended paper, "are among the fastest-growing segment of the IoT and promise to have widespread societal influences in the coming years, particularly in the areas of personal safety and security, health, wellness, fitness, personal organization, communication, and fashion."

If America hopes to be a global leader in wearable technologies, as it has been for the Internet more generally over the past two decades, then the country first has to get public policy right. America took a commanding lead in the digital economy because, in the mid-1990s, Congress and



the Clinton administration crafted a nonpartisan vision for the Internet that protected “permissionless innovation”—the idea that experimentation with new technologies and business models should generally be permitted without prior approval.

The first order of business for policymakers is to send a green light to entrepreneurs communicating that our nation’s default policy position remains “innovation allowed.” Second, policymakers should avoid basing policy interventions on hypothetical worst-case scenarios—or else best-case scenarios will never come about. Our policy regime, therefore, should be responsive, not anticipatory.

Of course, there exist privacy- and security-related challenges that deserve attention. Data is going to be moving fluidly across so many platforms and devices that it will be difficult to apply traditional Fair Information Practice Principles in a rigid regulatory fashion for every conceivable use of these technologies.

Specifically, it will be challenging to achieve perfect “notice and choice” in a world where so many devices are capturing volumes of data in real time. Moreover, while “data minimization” remains a worthy goal, if it is mandated in a one-size-fits-all fashion, it could limit many life-enriching innovations.

Law will still play a role, but we’re going to need new approaches.

- Policymakers can encourage privacy and security “by design” for wearable technology developers, but those best practices should not be mandated as top-down controls. Flexibility is essential.
- More privacy-enhancing tools—especially robust encryption technologies—will also help, and government officials would be wise to promote these tools instead of restricting them.
- Increased education is also essential, and governments can help get the word out about inappropriate uses of these technologies.
- Existing privacy torts and existing targeted rules (such as Peeping Tom laws) will also likely evolve to address serious harms as they develop.
- Finally, the Federal Trade Commission will continue to play an important backstop role, using its section 5 authority to police “unfair and deceptive” practices. The commission has already been remarkably active in encouraging companies to live up to the privacy and security promises they make to their consumers, and that will continue.

Thank you for the opportunity to submit this statement for the record. Policymakers should remain patient and continue to embrace permissionless innovation to ensure that wearable technologies thrive and American consumers and companies continue to be global leaders in the digital economy.

Sincerely,

Adam Thierer



**MERCATUS CENTER**  
George Mason University

Bridging the gap between academic ideas and real-world problems

## ECONOMIC PERSPECTIVES

### PROJECTING THE GROWTH AND ECONOMIC IMPACT OF THE INTERNET OF THINGS

Adam Thierer and Andrea Castillo

The next big wave of data-driven technological innovation will connect physical devices embedded with tiny computing devices to the Internet in an effort to seamlessly improve the measurements, communications, flexibility, and customization of our daily needs and activities. This “Internet of Things” (IoT) is already growing at a breakneck pace and is expected to continue to accelerate rapidly.

Adam Thierer of the Mercatus Center at George Mason University writes in a 2015 journal article that as is the case with any emerging technology, some groups have already started petitioning policymakers to limit or control IoT technologies out of fears of poor privacy or security outcomes. Policymakers are already investigating these issues. The Senate Committee on Commerce, Science, and Transportation recently held a hearing related to these issues, and in January the Federal Trade Commission (FTC) released a major report recommending a variety of privacy and security “best practices” for IoT. While some of these concerns are understandable, as Thierer writes in his 2014 book *Permissionless Innovation*, good public policy requires an appropriately weighted consideration of the projected benefits of any new development alongside the costs of regulatory interventions aimed at preemptively addressing perceived (and in some cases entirely hypothetical) fears.

In a testimony before the Senate Committee on Commerce, Science, and Transportation, Thierer highlighted that industry research groups have published several recent analyses that project the economic and social benefits of IoT technologies. While the methodologies, specific technologies analyzed, and final figures among these studies vary, they all indicate an industry consensus that the coming decades will be characterized by the introduction of billions of “smart” devices, millions of job opportunities, and trillions of dollars in economic growth and cost savings. The total number of connected devices in use globally—including such items as smart home appliances, “wearables,” smart metering systems, and autonomous vehicles—is projected to grow from 10 billion in 2013 to anywhere from 19 billion to 40 billion

*The ideas presented in this document do not represent official positions of the Mercatus Center or George Mason University.*

by 2019. The cost savings and productivity gains generated through “smart” device monitoring and adaptation are projected to create \$1.1 trillion to \$2.5 trillion in value in the health care sector; \$2.3 trillion to \$11.6 trillion in global manufacturing, and \$500 billion to \$757 billion in municipal energy and service provision over the next decade. The total global impact of IoT technologies could generate anywhere from \$2.7 trillion to \$14.4 trillion in value by 2025.

This summary provides a brief explanation of IoT technologies before describing the current projections of the economic and technological impacts that IoT could have on society. In addition to creating massive gains for consumers, IoT is projected to provide dramatic improvements in manufacturing, health care, energy, transportation, retail services, government, and general economic growth. Poorly considered policies should not prevent us from reaping these enormous benefits.

## WHAT IS THE INTERNET OF THINGS?

IoT, sometimes called “machine-to-machine” (M2M) communication technologies, is a series of networked “smart devices” that are equipped with microchips, sensors, and wireless communications capabilities. The underlying drivers of the Internet revolution—massive increases in processing power, storage capacity, and networking capabilities; the miniaturization of chips and cameras; and the digitization of data and assembly of “big data” repositories—have dramatically lowered the costs of integrating microchips, sensors, cameras, and accelerometers into everyday devices. Existing technologies and tools can be cheaply integrated with the Internet to engage with external information and react according to pre-programmed commands. The major categories of IoT technologies include “smart” consumer technologies, wearables, “smart” manufacturing and infrastructure technologies, and unmanned transportation.

### “Smart” Consumer Technologies

Consumer products will be designed with sensors and wireless capabilities to dynamically automate routine tasks. Mundane appliances that consumers have long taken for granted—like refrigerators, cooking devices, lights, and even weight scales—all will soon be networked, sensing, automated, and communicating as “smart” home technologies. Refrigerators are being designed to measure and record internal temperatures, monitor for bacteria or spoilage, and even keep track of food stocks to alert owners when supplies are running low—or just order a new delivery directly from the nearest grocery store’s website. Thermostats can already learn and adjust to household behavior and program themselves to save money on heating and cooling bills. Networked consumer products are expected to provide dramatic economic benefits by lowering the costs of household drudgery through automation, freeing up time for more productive activities, and extending the use and life of household goods by improving maintenance.

### Wearables

Wearables are a subset of consumer technologies that integrate networked devices into portable accessories like watches, jewelry, clothes, and glasses to collect data, track activities, and customize experiences to users' needs and desires. Wearable technologies are among the fastest-growing segment of the IoT and promise to have widespread societal influences in the coming years, particularly in the areas of personal safety and security, health, wellness, fitness, personal organization, communication, and fashion. Popular examples of wearables include fitness tracking and feedback products like Jawbone and FitBit that allow individuals to continuously measure and share daily fitness activities to isolate and improve their outcomes. Sophisticated wearable health devices will soon remind users to take medications or contact medical professionals as necessary and eventually help users track and even diagnose various conditions before advising a course of action. Other experiments with implantable "hearable" devices, "smart" contact lenses and glasses, and even tactile networked patches and fabrics seek to cheaply and seamlessly monitor other health vitals like blood glucose levels, blood pressure, brain activity, and stress. Dr. Eric Topol explains in his book *The Creative Destruction of Medicine* that these and other advances will improve preventative medicine and save billions of dollars in health care costs.

### "Smart" Manufacturing and Infrastructure Technologies

While flashy IoT applications to consumer technologies understandably generate the most media buzz, networked devices perhaps hold the most promise to cut costs and raise efficiency in production, manufacturing, and even traditional municipal waste services.

In this age of "Industry 4.0," factory managers will create networks of connected production facilities along entire value chains that can autonomously communicate with each other and direct changes in response to unexpected developments. Devices will provide constant, accurate measurements of output, resource depletion, and capital depreciation to isolate sources of waste and maximize factor productivity. Smart infrastructure technologies can allow government planners to measure and monitor traffic management, waste and water services, and even police services to lower costs and improve services for citizens. The dramatic improvements to marginal production and cost reduction in manufacturing wrought by IoT technologies are projected to generate billions in revenue growth and productivity over the next decade.

### Intelligent Vehicles and Unmanned Transportation

Adam Thierer and Ryan Hagemann of the Mercatus Center at George Mason University predict that networked vehicles and aircraft equipped with sensors, wireless communication, and dynamic programming will make unmanned transportation widely available and generate considerable benefits for consumers and manufacturing. "Autonomous vehicles" or "driverless cars" are automotive technologies that permit automobiles to operate without human assistance. Driverless cars are expected to dramatically reduce the number and costs of highway deaths and injuries while lowering the costs of shipping and transportation. Autonomous

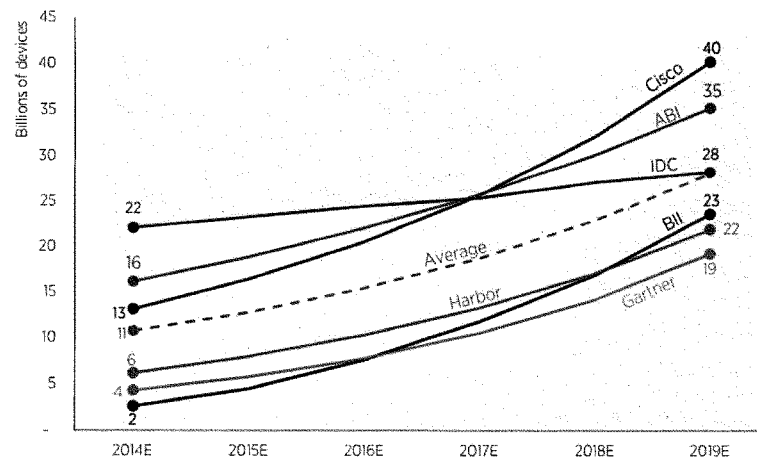
vehicles can also be used in manufacturing and warehouse capacities to improve speed and efficiency while lowering human injury and costs. Even short of fully autonomous systems, more “intelligent vehicle” technologies could produce significant social and economic benefits. On-board vehicle technologies are already an integral part of the expanding IoT universe. Experts at *Ars Technica* predict that “the automobile could be the first great wearable computer” and “your car might be the second most-used computing device you own before too long.”

Jerry Brito, Eli Dourado, and Adam Thierer of the Mercatus Center at George Mason University explain that “Unmanned aerial vehicles” (UAVs) or “Unmanned Aircraft Systems” (UASs), informally known as “drones,” employ similar networked concepts to automate aerial operations. UAVs will provide enormous productivity gains and cost savings in agricultural output, product delivery, and journalism and data gathering, as well as providing another exciting outlet as a good old-fashioned consumer hobby.

## PROJECTED TECHNOLOGICAL ADVANCEMENTS

Industry analyses of market trends anticipate robust growth in the total number of networked devices in use over the next decades. An estimated 10 billion wirelessly connected devices were already in use globally in 2013, according to ABI Research analysts. Similar research from other organizations provides a wide range of estimates of the total number of IoT devices anticipated to be in operation by 2019, from a low of 19 billion to an optimistic projection of 40 billion devices. These and other projections are discussed in more detail below.

Figure 1. Industry Estimates of Total Internet of Things–Connected Devices by 2019



Source: John Greenough, “The Internet of Things is Rising: How the IoT Market Will Grow Across Sectors,” *Business Insider Intelligence*, October 8, 2014. Produced by Adam Thierer and Andrea Castillo, Mercatus Center at George Mason University, 2015.

**Cisco projects** that 40 billion intelligent things will be connected and communicating by 2019.

**ABI Research** estimates that more than 35 billion networked devices will be in use by 2019.

**International Data Corporation (IDC)** predicts that around 28 billion networked devices will be in use by 2012 and that 212 billion devices will be connectable by 2020, 15 percent (around 31.8 billion) of which will be installed and operational by the end of 2020.

**Gartner** anticipates that 19 billion IoT devices will be in operation by 2019 and 25 billion devices will be online by 2020.

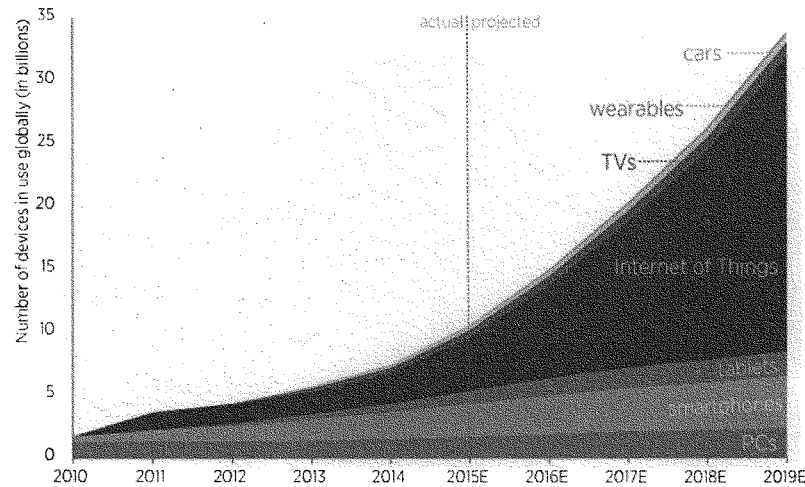
**Harbor** projects that 21.7 billion IoT devices will be connected and in use by 2019.

**Machina Research** reports that roughly 7.2 billion “machine-to-machine connected consumer electronic devices” will be in global use by 2023.

**Business Insider Intelligence (BII)** estimates that will be a total of 23.4 billion IoT devices connected by 2019 and that adoption will be driven by enterprise and manufacturing sectors.

Several analyses attempt to separate or isolate the total numbers within specific categories of IoT devices that will be connected over the next decade. Business Insider Intelligence provides historical and projected data on the number of installed IoT devices compared with PCs, smartphones, and tablets along with “smart” TVs, wearables, and “smart” cars (which are counted separately from IoT) from 2010 to 2019, which are displayed on the chart below. Growth in the number of installed IoT technologies is projected to exceed that of personal computers a factor of ten over the next four years, increasing from roughly 4.3 billion in 2015 to 23.4 billion by the end of 2019. Business Insider Intelligence anticipates that businesses will account for most of the growth in IoT-connected devices, projecting that almost 10 billion devices will be used in enterprise applications. “Smart” home, security, and energy devices will be another major consumer market and are projected to constitute almost 2 million of the total connected devices by 2019.

Figure 2. The Internet of Everything: Devices in Use Globally



Source: John Greenough, "The Internet of Everything 2015," *Business Insider Intelligence*. Produced by Adam Thierer and Andrea Castillo, Mercatus Center at George Mason University, 2015.

Other studies focus on specific market segments.

**Navigant Research** predicts that more than 1 billion smart meters will be installed globally by 2022, up from 313 million in 2013.

**ON World** projects that roughly 100 million Internet-connected wireless lights will be in operation by 2020.

**Business Insider Intelligence** projects that the annual number of wearables shipped will grow from 14.04 million in 2013 to 162.8 million in 2020, and that a total of 730.58 million wearable devices will be shipped throughout those years. Smartwatches are projected to lead the market, with 503.1 million devices projected to be shipped from 2013 to 2019, followed by fitness bands and activity trackers, projected at 168.9 million devices shipped, while another 58.54 million devices are projected to be shipped from remaining wearables markets. However, these projections were revised downwards from earlier BII projections anticipating shipments of more than 300 million devices by 2018 owing to persistent barriers to adoption and underwhelming market performance.

**IDC** analysts report that the global wearables market reached a total of 19.2 million devices in 2014 and project that the worldwide market will swell to 111.9 million networked devices sold in 2018.

**The International Federation of Robotics** reports that 806,000 connected industrial robots have been installed in manufacturing and shipping facilities and projects that roughly 2.6 million will be in operation by 2020.

**The Teal Group** estimates that the global civilian aerial drone market, worth roughly \$10 million in 2013, will grow by over 2,000 percent to reach \$2.2 billion in 2023.

**IHS Automotive** anticipates that the number of cars connected to the Internet will grow more than six fold from 2013 to reach 152 million internationally by 2020.

Industry projections present a vision of the future where billions of formerly dormant “things” actively sense, respond, and communicate with not only the people and environments but also other devices around them. The number of connected consumer devices—like wearables, TVs, and intelligent vehicles—will grow gradually but impressively. Smart appliances and climate control devices will become normal household objects in the coming decades. Networked manufacturing, production, and industrial delivery devices will largely drive the growth in the total number of IoT devices. We will now consider some of the economic benefits that will accompany these technological advancements.

## PROJECTED ECONOMIC BENEFITS

The growth in the total number of IoT devices is projected to provide substantial economic and social benefits in the way of cost savings, value creation, productivity improvements, and general economic growth. Improved industrial monitoring and automation techniques will help manufacturers and distributors to quickly pinpoint inefficiencies, minimize waste, and streamline processes. Consumer health measurement technologies will help to promote preventative health practices and identify risk factors while emergency response communications can provide near-instant care in life-threatening situations. Hospitals can cut down on costs through accurate patient monitoring and pharmaceutical management. “Smart” city technologies can help municipalities to improve service delivery and save resources through infrastructure monitoring and automatic optimization. Recent analyses of IoT technologies project these and other savings and productivity gains in agriculture, security, energy, retail, and resource extraction will amount to trillions in value over the coming decades.

**McKinsey Global Institute** researchers estimate the potential economic impact of IoT technologies to be \$2.7 trillion to \$6.2 trillion per year by 2025, the largest of which will be felt in the manufacturing and health care industries. By sector, IoT is projected to create each year:

- \$1.1 trillion to \$2.5 trillion in value in the health care sector
- \$0.9 trillion to \$2.3 trillion in value in manufacturing
- \$200 billion to \$500 billion in value in electricity provision



- \$100 billion to \$300 billion in value in urban infrastructure
- \$100 billion to \$200 billion in value in security provision
- \$100 billion to \$200 billion in value in resource extraction
- around \$100 billion in value in agriculture
- around \$50 billion in value in vehicle use

**Cisco analysts** estimate that IoT will create \$14.4 trillion in net profit between 2013 and 2022, which amounts to an increase in global corporate profits by roughly 21 percent. By sector, the “Value at Stake” generated by IoT is projected to be:

- \$1.95 trillion for manufacturing through “smart factory” techniques
- \$1.95 trillion for marketing and sales through location-based mobile advertising
- \$757 billion for municipalities through “smart grid” technologies
- \$635 billion for entertainment through connected gaming and media
- \$349 billion for infrastructure through “smart building” technologies
- \$347 billion for transportation through connected ground vehicles
- \$106 billion from health care through connected patient monitoring
- \$78 billion for education through connected private colleges

**General Electric** projects that industrial IoT technologies could add about \$15 trillion to global GDP by 2030 (in constant 2005 dollars) if they raise global annual productivity growth by 0.5 to 1 percentage points. Additionally, an estimated \$32.3 trillion in total global output can benefit from “Industrial Internet” technologies by optimizing information flows. The report estimates that the Industrial Internet opportunities of these sectors by 2025 will be:

- \$11.6 trillion in manufacturing
- \$7 trillion in health care
- \$4.8 trillion in transportation

**IDC** estimated in 2013 that IoT market would grow at a compound annual growth rate of 7.9 percent to reach \$8.9 trillion by 2020.

**Business Insider** estimates that IoT will add approximately \$5.6 trillion in value to the global economy in between 2014 and 2019, \$2.4 trillion of which will accrue to enterprise industry, \$1.7 trillion of which will accrue to government and municipal services, and \$1.5 trillion of which will accrue to home consumption.

**Accenture** estimates that the industrial IoT could add \$14.2 trillion to the global economy by 2030, and that the US economy will gain at least \$6.1 trillion in cumulative GDP by that year. If the US takes additional measures to employ IoT to improve domestic infrastructure, then Accenture projects that the gains to the US will rise to \$7.1 trillion over that same time. Another survey assembled by Accenture finds that 87 percent of the executives surveyed believe that IoT will result in long-term job growth.

**VisionMobile** projects that the number of IoT developers will grow from roughly 300,000 in 2014 to more than 4.5 million by 2020.

**Morgan Stanley** forecasts that driverless cars will save the US economy \$1.3 trillion per year once they fully penetrate the market, while saving the world another \$5.6 trillion a year. Specifically, they predict:

- \$507 billion in productivity gains
- \$488 billion in prevented accident costs
- \$158 billion in fuel cost savings
- \$138 billion in productivity gains from congestion prevention
- \$11 billion in fuel cost savings from congestion prevention

This growing body of research indicates that IoT will not just provide marginal consumer benefits and technological intrigue—it will change the industrial paradigm of the 21st century and can jump-start global economic productivity gains for decades to come.

## CONCLUSION

Recent projections of the economic and social benefits of networked IoT technologies suggest that their technological and economic impact will be significant. These analyses predict that tens or even hundreds of millions of networked devices will proliferate globally as industrial and infrastructure inputs, consumer wearables, smart home technologies, and automated transportation services. The economic gains in terms of cost savings and enhanced productivity growth are projected to be enormous. Trillions in value will be created through cost-savings through preventative health care, minimized accidents, patient monitoring, efficiencies in manufacturing and distribution, and seamless home and municipal infrastructure improvements.

These potentially large economic gains must be considered when policymakers are debating policy for IoT. It is always easy to conjure up hypothetical worst-case scenarios about how some of these technologies may be misused, or how they might disrupt certain sectors and professions. But, as Thierer writes, if public policy is based upon fear of worst-case scenarios, then best-case scenarios will never come about. As economic historian Joel Mokyr has observed, “technological progress requires above all tolerance toward the unfamiliar and the eccentric.” More generally, long-term social progress and economic prosperity hinge upon a general willingness to engage in ongoing trial-and-error experimentation with new technologies like IoT.

Policymakers should carefully weigh the costs associated with any proposed IoT regulations against the enormous projected benefits: both in the short term and long term. Smart technologies require smart regulations.

---

#### CONTACT

Taylor Barkley, 703-993-8205, [tbarkley@mercatus.gmu.edu](mailto:tbarkley@mercatus.gmu.edu)  
 Mercatus Center at George Mason University  
 3434 Washington Boulevard, 4th Floor, Arlington, VA 22201  
[www.mercatus.org](http://www.mercatus.org)

---

#### ABOUT THE AUTHORS

Adam Thierer is a senior research fellow with the Technology Policy Program at the Mercatus Center at George Mason University. He specializes in technology, media, Internet, and free-speech policies, with a particular focus on online safety and digital privacy. His latest book is *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*. Thierer is a frequent guest lecturer, has testified numerous times on Capitol Hill, and has served on several distinguished online safety task forces, including Harvard University’s Internet Safety Technical Task Force and the federal government’s Online Safety Technology Working Group. He received his MA in international business management and trade theory at the University of Maryland.

Andrea Castillo is the program manager of the Technology Policy Program for the Mercatus Center at George Mason University and is pursuing a PhD in economics at George Mason University. She is a coauthor of *Liberalism and Cronyism: Two Rival Political and Economic Systems* with Randall G. Holcombe and *Bitcoin: A Primer for Policymakers* with Jerry Brito. Castillo received her BS in economics and political science from Florida State University.

---

#### ABOUT THE MERCATUS CENTER

The Mercatus Center at George Mason University is the world’s premier university source for market-oriented ideas—bridging the gap between academic ideas and real-world problems.

A university-based research center, Mercatus advances knowledge about how markets work to improve people’s lives by training graduate students, conducting research, and applying economics to offer solutions to society’s most pressing problems.

Our mission is to generate knowledge and understanding of the institutions that affect the freedom to prosper and to find sustainable solutions that overcome the barriers preventing individuals from living free, prosperous, and peaceful lives.

Founded in 1980, the Mercatus Center is located on George Mason University’s Arlington campus.

[www.mercatus.org](http://www.mercatus.org)

## Uncle Sam Wants Your Fitbit

**The fight for Internet freedom gets physical.**

Adam Thierer | Apr. 9, 2015 9:00 am

We are at the dawn of the Internet of Things—a world full of smart devices equipped with sensors, all hooked up to a digital universe that will become as omnipresent as the air we breathe. Imagine every appliance in your home, every machine in your office, and every device in your car constantly communicating with a network and offering you a fully customizable, personalized experience. Besides neat gadgets and productivity gains, this hyper-connected future will also mean a new wave of policy wars, as politicians panic over privacy, security, intellectual property, occupational disruptions, technical standards, and more.

Behind these battles will be a grander clash of visions over the future course of technology. The initial boom of digital entrepreneurship was powered by largely unfettered experiments with new technologies and business models. Will we preserve and extend this ethos going forward? Or will technological reactionaries pre-emptively eliminate every hypothetical risk posed by the next generation of Internet-enabled things, perhaps regulating them out of existence before they even come to be?

### Web Wars

The first generation of Internet policy punditry was dominated by voices declaring that the world of bits was, or at least should be, a unique space with a different set of rules than the world of atoms. Digital visionary John Perry Barlow set the tone with his famous 1996 essay, "A Declaration of the Independence of Cyberspace," which argued not just that governments should leave the Internet unregulated but that Internet regulation was not really feasible in the first place.

Barlow's vision thus embodied both *Internet exceptionalism* and *technological determinism*. Internet exceptionalism is the notion that the Net is a special medium that shouldn't be treated like earlier media and communications platforms, such as broadcasting or telephony. Technological determinism is the belief that technology drives history, and (in the extreme version) that it almost has an unstoppable will of its own.

First-generation exceptionalists and determinists included Nicholas Negroponte, the former

director of the MIT Media Lab, and George Gilder, a technology journalist and historian. "Like a force of nature, the digital age cannot be denied or stopped," Negroponte insisted in his 1995 polemic, *Being Digital*. But Barlow's declaration represented the high-water mark of the early exceptionalist era. "Governments of the Industrial World," he declared, "are not welcome among us [and] have no sovereignty where we gather." The "global social space we are building," he added, is "naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear."

It turned out we had reasons to fear after all. If the first era of Internet policy signified *A New Hope*, the second generation—beginning about the time the dot-com bubble burst in 2000—could be called *The Empire Strikes Back*. From taxes to surveillance to network regulation, governments gradually learned that by applying enough pressure in just the right places, citizens and organizations will submit.

A second generation of Internet scholars cheered on these developments. The scholar-activists at Harvard's Berkman Center for Internet and Society, such as Lawrence Lessig, Jonathan Zittrain, and Tim Wu, joined with a growing assortment of policy activists with tangential pet peeves they wanted governments to address. Together they revolted against the earlier ethos and called for stronger powers for governments to direct social and commercial activities online.



Mark Rightmire / The Orange  
County Register /  
ZUMAPRESS.com

In the new narrative, the real threat to our freedom was not public law but private code. "Left to itself," Lessig famously predicted, "cyberspace will become a perfect tool of control." Thus, government controls were called for. Later, Wu would advocate a forcible disintegration of the information economy via a "separations principle" that would segregate information providers into three buckets—creators, distributors, and hardware makers—and force them to stay put. All in the name of keeping us safe from "information monopolies."

Spurred on by this crowd, governments across the globe are clamoring for even greater control over people in cyberspace. But the second generation's narrative has proved overly simplistic in two ways.

First, the exceptionalists and techno-determinists were partially right—the Internet, while not being unregulatable per se, really has proven more resistant to government

control than analog-era communications systems. The combination of highly decentralized networks, a global scale, empowered end-users, and the unprecedented volume of information created in the process has created formidable enforcement challenges for would-be censors and economic regulators.

With each passing year, the gap between "Internet time" and "government time" is widening. As the technology analyst Larry Downes argued in his 2009 book *The Laws of Disruption*, information-age "technology changes exponentially, but social, economic, and legal systems change incrementally." His examples ranged from copyright law, where bottling up published works is growing harder, to online privacy, where personal information is flowing faster than the ability of the law to control it.

This leads to the second way in which the *Empire Strikes Back* narrative falls short. As the Internet changes the way people connect with one another, governments have had to change the way they try to impose their wills on the rest of us. The old command-and-control models just don't work on highly distributed and decentralized networks.

Consider regulation of speech. Outright censorship has proven extremely difficult to enforce, and not just in the United States, where we have a First Amendment keeping the police at bay. Although some atavistic regimes still try to clamp down on content and communications, most attempt to shape behavior by encouraging firms and organizations to adopt recommended codes of conduct for online speech, often in the name of protecting children.

A similar phenomenon is at play for data privacy and cybersecurity policy. While some comprehensive regulatory frameworks have been floated, the conversations are shifting toward alternative methods of encouraging compliance. Many governments are choosing the softer road of encouraging codes of conduct and "best practices."

Economic regulations have evolved, too. Price and entry controls are almost never suggested as a first-order solution to concerns over market concentration. Instead of hard-nosed, top-down diktats, governments are increasingly using "nudges," convening "multistakeholder" meetings and workshops, and deploying what Tim Wu calls "agency threats." The Obama administration's Commerce Department and Federal Trade Commission (FTC) have already used this approach in their attempts to influence "big data" collection, biometrics, online advertising, mobile app development, and other emerging sectors and technologies.

Think of it as a "soft power" approach to tech policy: Policy makers dangle a regulatory Sword of Damocles over the heads of Internet innovators and subtly threaten them with vague penalties—or at least a lot of bad press—if they don't fall into line. The sword doesn't always have to fall to be

effective; the fact that it's hanging there is enough to intimidate many firms into doing what regulators want. It's similar to the approach that the Food and Drug Administration has employed for decades with many food or medical device manufacturers: constantly harping on them about how to better develop their products, often without ever implementing formal regulations clarifying exactly how to do so.

That's how policy makers are already approaching the Internet of Things, too.

### **Why Matter Matters**

It may feel like the Internet is already a ubiquitous backdrop of our existence, but "getting online" still requires a conscious effort to sit in front of a computer or grab a smartphone and then take steps to connect with specific sites and services. The Net does not have a completely seamless, visceral presence in our everyday lives. Yet.

The Internet of Things can change that, ushering in an era of ambient computing, always-on connectivity, and fully customizable, personalized services. Wearable health and fitness devices like Fitbit and Jawbone are already popular, foreshadowing a future in which these devices become "lifestyle remotes" that help consumers control or automate many other systems around them—in their homes, offices, cars, and so on.

Nest, recently acquired by Google, is already giving homeowners the ability to better manage their homes' energy use and to do so remotely. It signals the arrival of easy-to-program home automation technologies that will, in short order, allow us to personalize nearly every appliance in our home.

Meanwhile, our cars are quickly becoming rolling computers, loaded with chips and sensors that automate more tasks and make us safer in the process. Soon, automobiles will be communicating not only with us but with everything else around them. While fully driverless cars may still be a few decades away, semi-autonomous technologies that are already here are gradually making it easier for our cars to drive us instead of us driving them.

Think of this new world as the equivalent of Iron Man Tony Stark's invisible butler JARVIS; we'll be able to interface with our devices and the entire world around us in an almost effortless fashion. Apple's Siri and similar digital personal assistants are already on the market but are quite crude. The near future will bring us Siri's far more advanced descendants, ambient technologies that are invisible yet omnipresent in our lives, waiting for us to bark out orders and then taking immediate, complex actions based on our demands.

After that we may quickly enter the realm of cyberpunk. There are already plans for "digital skin" and "electronic tattoos" that affix ultrathin wearables directly to the body. Many firms have already debuted "epidermal electronics" that, beyond the obvious health monitoring benefits, will allow users to interface with other devices—money scanners might be one obvious application—to allow frictionless transactions. Monitoring and communication technologies could also be swallowed or implanted within the body, allowing users to develop a more robust and less invasive record of their health at all times.

These innovations are poised to fuel an amazing transformation in the industrial world too, leading to a world of machine-to-machine communications that can sense, optimize, and repair instantaneously, producing greater efficiency. Consulting firms such as McKinsey and IDC have predicted that this transformation will yield trillions of dollars' worth of benefits by expanding economic opportunities and opening up new commercial sectors.

When the Net is being baked into everything we contact, policy anxieties will multiply rapidly as well. Security and privacy concerns already dominate policy discussions about the Internet of Things. Critics fear a future in which marketers or the government scrape up the data our connected devices will collect about us. But even more profound existential questions are being raised by legal theorists, ethical philosophers, and technology critics, who often conjure up dystopian scenarios of intelligent machines taking over our lives and economy.

#### **Which Vision Shall Govern?**

This is where the question of permissionless innovation comes into play. Will Internet of Things-era innovators be at liberty to experiment and to offer new inventions without prior approval? Or will a more precautionary approach prevail, one where creators will have to get the blessing of bureaucrats before launching new products and services?

The FTC has already issued reports proposing codes of conduct to manage the growing deluge of data. The goal is to encourage coders to bake in "privacy by design" and "security by design" at every step of product development. In particular, FTC officials want developers to provide users with adequate notice regarding data collection practices, while also minimizing data collection in the aggregate.

Many of those practices are quite sensible as general guidelines, especially those related to promoting the use of encryption and anonymization to better secure stored data. But the FTC wants developers *always* to adopt such privacy and data security practices, and it wants to be able to hit them with fines and other penalties (using the agency's "unfair and deceptive practices" authority) if they fail to live up to those promises. If the intimidation game gets too



aggressive and developers reorient their focus to pleasing Washington instead of their customers, it could have a chilling effect on many new forms of data-driven, Internet-enabled innovation.

The FTC has already gone after dozens of digital operators in this way, including such Internet giants as Google. In consent decrees, the commission extracted a wide variety of changes to those companies' privacy and data collection practices while also demanding that they undergo privacy audits for a remarkable two decades. That'll provide regulators with a hook for nudging corporate data decisions for many years to come.

While the FTC looks to incorporate the Internet of Things within this expanded process, some precautionary-minded academics are pushing for even more aggressive interventions. Many critics of private-sector data collection would like to formalize the FTC's privacy and security auditing process. Decrying a supposed lack of transparency regarding the algorithms that power various digital devices and services, they propose that companies create internal review boards or hire "data ethicists" (like themselves) to judge the wisdom of each new data-driven innovation before product launch.

More far-reaching would be the "algorithmic auditing" proposed by tech critic Evgeny Morozov and others. Advocates seek a legal mechanism to ensure that the algorithms that power search engines or other large-scale digital databases are "fair" or "accountable," without really explaining how to set that standard. There's also a movement afoot for some sort of "right of reply" to protect our online reputations by forcing digital platforms to give us the chance to respond to websites or comments we don't like. The European Union is already going down this path with the so-called Right to be Forgotten law, which mandates that search results for individuals' names be scrubbed upon request.

Fortunately, we are protected from such mandates in the U.S. by the First Amendment. The right to code is the right to speak. Technocrats will have to be cleverer to impose their controls stateside. Realizing that those roadblocks lie ahead, some activists are already trying to shift the discussion by claiming it's about "civil rights" and the supposed disparate impact that will occur if algorithmic decisions are left to the marketplace. Danielle Keats Citron, a law professor at the University of Maryland, calls for "technological due process" that would subject private companies to the sort of legal scrutiny usually reserved for government actors.

Meanwhile, new bureaucracies are being floated to enforce it all. Apparently the alphabet soup of technocratic agencies already trying to expand their jurisdictions to cover emerging technologies —FCC, FTC, FDA, FAA, NHTSA, etc.—aren't doing enough for the critics. For example, Frank Pasquale, also of Maryland's law school, favors not only a right of reply but also a Federal Search Commission to oversee "search neutrality" (think of it as net neutrality for search engines and

social networking sites), as well as "fair automation practices" that would regulate what he regards as the "black box" of large private databases. And Ryan Calo of the University of Washington School of Law fears "digital market manipulation" that might "exploit the cognitive limitations of consumers." He also proposes a Federal Robotics Commission "to deal with the novel experiences and harms robotics enables."

### **Better Safe Than Sorry?**

Anticipatory regulatory threats such as these will proliferate in tandem with the expanding penetration of ambient, networked technologies. The logic that animates such thinking has always been seductive among the wet-blanket set: Isn't it better to be safe than sorry? Why not head off hypothetical problems in privacy and security?

There is no doubt that slowing Internet of Things development could prevent future data spills or privacy losses, just as there is no doubt that regulatorily strangling Henry Ford's vision in the crib would have prevented numerous car crashes (while also preventing all the advantages cars have brought to our lives as well). If we spend all our time worrying over worst-case scenarios, that means the *best-case* scenarios will never come about either. Nothing ventured, nothing gained.

The trans-Atlantic contrast between the U.S. and Europe on digital innovation over the past 15 years offers real-world evidence of why this conflict of visions matters. America's tech sector came to be the envy of the world, and many U.S.-based firms are household names across Europe. (Indeed, European regulators are constantly trying to take the likes of Google, Amazon, and Facebook down a peg.) Meanwhile, it is difficult to name more than a few major Internet innovators from Europe. America's more flexible, light-touch regulatory regime left more room for competition and innovation compared to Europe's top-down regime of data directives and bureaucratic restrictions.

Instead of precaution, a little patience is the better prescription. Long before the Internet of Things came along, many predecessor technologies—telephones, broadcast networks, cameras, and the Net itself—were initially viewed with suspicion and anxiety. Yet we quickly adapted to them and made them part of our daily routines.

Human beings are not completely subservient to their tools or helpless in the face of technological change. Citizens have found creative ways to adjust to technological transformations by employing a variety of coping mechanisms, new norms, or other creative fixes. Historically, the births of new, highly disruptive networking technologies—think of social networking sites just a decade ago—have been met by momentary techno-panics, only to see citizens quickly adapting to them and then clamoring for more and more of the stuff. The same

will be true as we adjust to the Internet of Things.

If we hope to usher in what Michael Mandel, chief economic strategist at the Progressive Policy Institute, calls "the next stage of the Internet Revolution," we'll need to guarantee that innovators will remain free to experiment with new and better ways of doing things. That's the Internet freedom we should be fighting for.

FRED UPTON, MICHIGAN  
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY  
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON ENERGY AND COMMERCE  
2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115  
Majority (202) 225-2927  
Minority (202) 225-3641  
March 22, 2016

Mr. Thomas D. Bianculli  
Vice President, Enterprise Technologies Office  
Zebra Technologies  
3 Overlook Point  
Lincolnshire, IL 60069

Dear Mr. Bianculli,

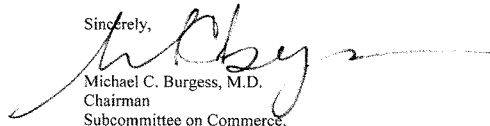
Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Thursday, March 3, 2016, to testify at the hearing entitled "Disrupter Series: Wearable Devices."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Tuesday, April 5, 2016. Your responses should be mailed to Giulia Giannangeli, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to [Giulia.Giannangeli@mail.house.gov](mailto:Giulia.Giannangeli@mail.house.gov).

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

  
Michael C. Burgess, M.D.  
Chairman  
Subcommittee on Commerce,  
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

Attachment



Zebra Technologies  
Enterprise Corporation  
1 Zebra Plaza  
Holtsville, NY 11742

p 800-722-6234  
f 631-738-3246  
zebra.com

April 4, 2016

Ms. Giulia Giannangeli  
Legislative Clerk  
Committee on Energy and Commerce  
2125 Rayburn House Office Building  
Washington, DC 20515

Dear Ms. Giannangeli:

Attached please find my responses to the written questions posed by Chairman Burgess and Congressman Harper relative to the Subcommittee's March 3 hearing on wearable technology.

I thank the Subcommittee for the opportunity to testify and present the views of Zebra Technologies Corporation on this very important issue. My company and I look forward to continuing to work with the Subcommittee on issues of mutual interest and I invite you to be in contact anytime we may be of assistance.

Sincerely,

Thomas D. Bianculli  
Vice President, Emerging Technology Office  
Zebra Technologies Corporation

The Honorable Michael C. Burgess, M.D.

**1. *Currently, are there any regulatory challenges at the Federal, State, or local level facing businesses that impede the use of wearables in workplace?***

The primary challenge we believe policymakers face is to foster an environment that supports the rapid development, deployment and subsequent advancement of wearables in a manner that simultaneously addresses concerns over data security, encryption and privacy. The goal must be to encourage technologies which provide enhanced, secure and real-time visibility and access to information in a way that empowers workers to undertake more effective and timely decisions and actions. It is for this reason that we urge Congress and the Administration to take a light touch where wearable technology is concerned – for the same reasons that many in industry as well as in Congress and the Administration have advocated for a light regulatory approach to the Internet of Things (IoT).

Inherent in our view is our appreciation for the fact that issues attendant to Business-to-Business (B2B) and Business-to-Government (B2G) applications of wearable technologies can differ – in some or many instances – from the issues which arise in a Business-to-Consumer (B2C) setting or context. This means that policymakers can benefit from viewing IoT-based technologies like wearables in all settings, whether B2B, B2C or B2G.

Zebra's suite of enterprise wearable technologies represents a series of solutions purposely built to solve complex problems in the B2B and B2G space. We deliver design innovations driven by deep customer insight. We have an unmatched research and study capabilities which enable us to immerse ourselves deeply into the B2B and B2G end user experience and help guide how users engage technology and receive information. Real-world analysis, a vast collection of field research, deep experiential immersion, and voice of customer insights all represent key front-end parameters of our design research approach. Ergonomics, cognitive and clinical psychology, and physical and cultural anthropology are integrated into design process to deliver intuitive user experiences in the B2B and B2G spaces that enhance situational awareness and provide critical info for improved decision making. We match the design approach with engineering regulatory and industry standards and practices to deliver best-in-class enterprise tools. Our "outside-in" perspective is crucial; we conduct focused B2B and B2G customer research, trials and pilots by immersing our teams into our customers' worlds to prove the safety and efficacy of not just our wearable but our entire line of technology solutions we deliver to market.

**2. *How reliable are wearable devices in gathering information and presenting an accurate picture of the individual's performance or job execution?***

Enterprise wearable devices are purpose-built B2B and B2G devices designed to solve specific business and operational problems. For example, in the B2B space, customers have deployed Zebra's wearable devices to reliably find, route and track packages through global supply chains, bringing products to our stores and doorsteps. Zebra is currently exploring new and emerging component technologies to bring a new batch of wearable technologies to market – ones that help bring eye-level business-critical information to a worker without interrupting workflow. Zebra feels these newer technologies help create a frictionless experience which helps improve both individual performance efficiency and overall macroeconomic productivity.

By way of background, Zebra pioneered the industrial B2B wearable product category back in 1992 with

the introduction of a wrist mounted computer and finger ring scanner accessory for the logistics and transportation industry as an easier way to find and pick parcels faster in warehouses. We reduced friction in the workflow which has helped save businesses time and money while automating tasks for those on the front line. Fast forwarding to today, hundreds of thousands of these devices are helping to ship and track our online orders to our homes.

Moving forward, we see an ever-growing need for future global workforces to operate in a hands-free environment, literally focusing on the task at hand. It is for this reason that we launched our hands-free, head-mounted computer in 2013. It provides a wireless, hands-free wearable mobile computer that uses simple voice commands and head gesture controls to access complex data, video and voice and is geared towards field technicians using it for real-world business applications in tough environments – whether they're in a tight space, in a remote location or working high above the ground.

**3. *What types of information can business collect from wearables in manufacturing? And how would a business turn that information into actionable data that can help them improve workflows either in the factory or in a remote location to increase productivity?***

Wearable technology represents explosive future growth in manufacturing, both in terms of final products and ingredient technology components. This means that supply chains will grow with the availability and introduction of more innovative and new wearable technologies that solve end-user problems across the B2B, B2G and B2C sectors. Wearable technology will also grow with the continued availability and accessibility of affordable 3D printing, micro computing components, and open development platforms.

All of this reflects the fact that people across many different industries need the use of their hands to fix machines, heal patients and help customers and taxpayers. Many companies see users of wearable technology as warehouse workers picking real-time orders; field technicians responsible for the maintenance and repair of complex machines and vehicles; construction managers and architects who access schematics, building plans and maps; and military, medical and public safety teams who practice simulated training, live events and crisis scenarios.

In essence, wearable technology enhances situational awareness by giving people access to critical data and real-time video at the point of work. Imagine having full access to your business critical data – maps, grid schematics, and work tickets – as well as key engineers and experts – in full view whenever you need it with a simple verbal command. And then using another verbal command, you will be responding to and transmitting pictures or data updates back to the main office. Now imagine having that ability while suspended high above the ground repairing live electrical wires or working inside an airplane engine. No hands required. Wearable technology makes it happen.

**4. *What kinds of cost savings can manufacturers achieve through employee use of wearable devices and in what areas of a manufacturer's operational responsibilities do you tend to see most of those savings? How do those cost savings achieved through wearable devices translate into economic benefits for the U.S. economy at large?***

Manufacturing and field service will experience a significant and positive increase in performance from wearable technology adoption. Enhancing an already highly-skilled, technical workforce with tools that bring greater value to professional services and service-level agreements will, in turn, yield macroeconomic gains in productivity that will help contribute to enhanced national prosperity.

These benefits occur because wearable technology enables real-time collaboration that, in turn, reduces costs and improves operational quality. Wireless technology is making it easier for enterprises to change how they work, particularly in manufacturing and field service. The ability to communicate instantly and hands-free with subject matter experts regardless of location helps mobile workers increase productivity and resolve issues quickly and cost-effectively. It allows people to work smarter and safer; to keep their eyes literally focused on the task at hand. With full voice, audio, video, wireless and PC networking capabilities, Zebra's wearable technology portfolio gives enterprise users powerful new tools to transform how work gets done.

For example, when on a job site, enterprise workers need access to critical information and the ability to connect to subject matter experts at various locations in real-time to solve issues at the point of work. This is particularly important in environments where response time, accuracy and safety are key business factors. In the automotive manufacturing, the nuclear and utility industries, work protocols require a concise list of safety checks that must be completed on a daily basis. The steps are so important that they must be viewed and verified by at least two technicians. Mobile computing solutions that allow workers to collaborate easily, complete tasks accurately and keep their risk of exposure to a minimum can also eliminate the need for two additional technicians to be onsite. Real-time video gives them the ability to see what a worker sees and immediately verify job performance from anywhere. Every day, EMTs require direct communication with doctors and specialists at surrounding hospitals, to help care for critically injured or ill patients. Collaborating hands-free reduces errors and saves valuable time. Wearable technology devices in this environment need to enable reliable, interactive communications and stand up to the rigors of both indoor and outdoor use.

#### **The Honorable Gregg Harper**

##### ***1. What enhanced capabilities do you see wearable devices providing in the next five to 10 years, beyond what they are providing to consumers and businesses today?***

Future wearable computing in the B2B and B2G space will evolve into both all-in-one computing solutions and distributed solutions. As a result, they will be more reliant on both personal and body-area networks. For example, future hazard or safety sensors worn on equipment such as utility worker vests and scanner gun holsters may migrate away from being individual devices and become incorporated into a field engineer's and first responder's everyday gear and clothing so that frontline personnel are not encumbered by the technology. Visual computing, or the ability to work hands-free while receiving eye-level information, will be an impactful paradigm shift in how we, as humans, directly interface with computers. Visual computing delivering hands-free, eye-level information will enable frictionless, uninterrupted workflow.

Over the next few years, wearable devices will get smaller with miniaturization and technological improvements in battery technologies. It may be too early to see biologically embedded or implantable devices, but more integrated devices using sensors that can enhance, monitor or tap into body signs are on the horizon. Many companies will create their own wearable technologies, creating a variety of different technology platforms and user experiences. The use of standard protocols such as Bluetooth and Wi-Fi will enable more wearable devices and peripherals to more easily talk to each other.



We see computing, in general, moving faster into cloud-based networks. Future wearable devices will become more about context and situational awareness – autonomously gathering visual and audio data – synthesized in the cloud and relaying back relevant information to the wearable technology user. Today's devices will become more integrated, giving rise to unique and highly personalized systems. Wearables will become pervasive in the future, from conformable displays and eye-level user interfaces to self-forming sensor networks. The ecosystem created by wearables will require robust secure communications and power management needs. New security methods will also be necessary to keep hackers from controlling home appliances and business machines and devices.

Looking forward into the distant future, Zebra anticipates even more integration between man and machine. Brain to computer interfaces will open new possibilities to amputees controlling smart prosthetics, even ways for patients with no motor physical skills to communicate and be part of our connected world. Future battery technologies will harvest energy from our bodies, ambient noise, Wi-Fi, and air, powering next-gen bionics as well as other wearable, implantable devices.

**2. *What does this fast pace of innovation mean for policymakers in terms of how we should be thinking about the technology?***

The Internet of Things (IoT) is all around us. Wearable technologies, like all other technologies, will need to take advantage of the connectivity that the IoT provides. Zebra has created an IoT application enablement platform that allows organizations to easily and securely connect all types of devices, equipment and sensors to the Internet. Our company's platform approach helps organizations achieve economies of scale by taking full advantage of the data and information they generate to grow their operations, increase efficiency and drive productivity.

Most immediately, we urge Congress and the Administration to avoid ad hoc action that burdens the development and deployment of the IoT – and related IoT-technologies such as wearables – until a coordinated approach across the Administration has been developed. We respect why many in government want to make sure that subject-specific concerns are addressed as IoT-based technologies like wearables are developed and deployed but we believe a coordinated, government-wide approach would be far more efficient and supportive of the proper development of IoT-based technologies.

Crucial factors are at play that will radically transform the face of today's government and business workforces, including:

- The ability to coordinate mission-critical and business-critical communications within and across organizations;
- A flood of information available to individuals for better decision making; and
- The need to do more with less and do it in a manner that is better, faster and smarter.

We must continue innovating for the next generation of needs and opportunities in the B2B, B2G and B2C markets, working with customers and technology partners to develop meaningful solutions that elevate the user experience and help American workers to be the best at what they do. We must continue our deep commitment to research and development, strengthening our position at the forefront of technology to guide future innovations like wearable technology and, ultimately, transform the industries of the future. Congress' permanent extension of the R&D Tax Credit last year was very much a step in the right direction.

FRED UPTON, MICHIGAN  
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY  
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON ENERGY AND COMMERCE  
2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115  
Majority (201) 225-2921  
Minority (202) 225-3641  
March 22, 2016

Ms. Meg Burich  
Director of Commercial Development and Marketing  
Adidas Digital Sports  
4 Hillman Drive  
Chadds Ford, PA 19317

Dear Ms. Burich,

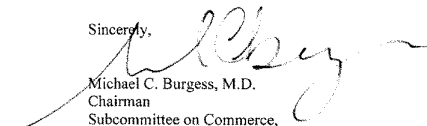
Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Thursday, March 3, 2016, to testify at the hearing entitled "Disrupter Series: Wearable Devices."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Tuesday, April 5, 2016. Your responses should be mailed to Giulia Giannangeli, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to [Giulia.Giannangeli@mail.house.gov](mailto:Giulia.Giannangeli@mail.house.gov).

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

  
Michael C. Burgess, M.D.  
Chairman  
Subcommittee on Commerce,  
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

Attachment

[Ms. Burich did not answer submitted questions for the record by the time of printing.]

FRED UPTON, MICHIGAN  
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY  
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON ENERGY AND COMMERCE  
2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115  
Majority (202) 225-2927  
Minority (202) 225-3601  
March 22, 2016

Mr. Suresh Palliparambil  
American Sales and Business Development Director  
NXP  
411 East Plumeria Drive  
San Jose, CA 95134

Dear Mr. Palliparambil,


Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Thursday, March 3, 2016, to testify at the hearing entitled "Disrupter Series: Wearable Devices."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Tuesday, April 5, 2016. Your responses should be mailed to Giulia Giannangeli, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to [Giulia.Giannangeli@mail.house.gov](mailto:Giulia.Giannangeli@mail.house.gov).

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

  
Michael C. Burgess, M.D.  
Chairman  
Subcommittee on Commerce,  
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

Attachment



April 18, 2016

United States House of Representatives  
 The Honorable Michael C. Burgess, Chairman  
 The Honorable Jan Schakowsky, Ranking Member  
 Committee on Energy and Commerce - Subcommittee on Commerce, Manufacturing, and Trade  
 2125 Rayburn House Office Building  
 Washington, DC 20515

**Re: response to additional questions**

Dear Chairman Burgess, dear Ranking Member Schakowsky,

With regard to the additional questions presented in connection with my recent testimony in the "Disruptor Series" on wearable technology, I wish to present for your consideration the following responses. The original questions are included below.

***Questions presented by Congressman Burgess:***

1. **What are the biggest challenges that you've seen to businesses and consumers in the adoption of wearable devices?**

Response:

Challenges to consumers are less than with businesses as this is where the primary adoption of wearables is today. But if you compare wearable adoption to that of something like smartphones, there is a long way to go before we can consider wearables mainstream. This is attributed to the usefulness of the wearable in moving beyond just a simple activity tracker to either something that is a great extension of the smartphone, or can stand alone in the eyes of the user. Adding features such as alarms and messaging that extends from the smartphone to the wearable, bringing price points down, and enhancing the industrial design appeal of wearables are all factors that support the expansion of the market. Businesses are adopting wearables either as extensions of their health care plans, to get their employees fit, or as perks to enhance the social aspect of team challenges. With either business or consumer, security and privacy are central points of much of the buying criteria.

2. **Mr. Palliparambil, given NXP's presence in many of the wearable devices on the market today, do we currently have the infrastructure to support the rapidly growing wearables market and accommodate multiple users? If not, where do we need to see greater support and investment to help drive this market forward?**

Response:

Two things were catalysts for wearables to emerge, the smartphone and the cloud, so we certainly do have the infrastructure to support the growth of wearables. What we lack is standards that are enforcing best practices, such as authentication of data at rest or in transit, encryption of the same data to ensure user privacy. As we can see with smart devices today, there are always actors with malicious intent whether to inflict financial harm or just to burden others for fun, which in turn means that we should be mindful of this from the creation of a wearable to delivery of the same to the consumers, and what we need to protect against.

3. **What do you think is the most significant cybersecurity concern facing wearable devices and how is NXP addressing it?**

Response:

Cybersecurity is broad reaching and the risks of wearables is in how they can be utilized. Imagine a wearable that is used as an activity tracker and also to unlock one's home. This would be more of a target to hackers because they will get personal data on the user that could indicate when they are away from home and also the keys to the home, such that a burglar can have easy access with lower risk of getting caught. This is just one extreme example, where another less extreme is a hacker posts the users wearable data online in public, and an insurance company gets ahold of the data and then uses it to change the premiums for a user, or even worse, deny coverage.

***Questions presented by Congressman Harper:***

1. **What enhanced capabilities do you see wearable devices providing in the next five to 10 years, beyond what they are providing to consumers and businesses today?**

Response:

Much like smartphones, wearables will continue to see evolutions thru the benefits of semiconductor integration and innovation followed by enhance software evolutions such as Android and iOS. Similar features on smartphones can find their way to wearables and thus untether the wearable from the smartphone, making it a standalone device. We already see cellular connectivity on wearables today in 2016 as an example of this

trend. Pricing and usefulness of these extra features will keep this transition on a slow pace in the interim, but in 5-10 years, all bets are off as one can see the drastic changes in smartphones that happened in the same short period.

**2. What does this fast pace of innovation mean for policymakers in terms of how we should be thinking about the technology?**

Response:

Policy makers also benefit from innovation both as consumers and business owners. These wearable enhancements can drive a more physically fit work force, which in turn can lead to more productivity. The ability to make ourselves smarter about our own health and fitness can allow us to make better choices faster. The caveat is that the privilege of this information is what is important and this is where policy makers can make a mark, but advocating for the users and balancing the relationship of this data between the user and the business. As we move to a smarter world with wearables and the Internet of Things, we need to lay down a foundation that encourages innovation while ensuring some boundary conditions around security and privacy are well established principles of the industry.

On behalf of NXP Semiconductors, I again thank you for the opportunity to present the company's views and hope that the foregoing responses are adequate and helpful. I welcome further questions at any time.

Respectfully,



Suresh Palliparambi

FRED UPTON, MICHIGAN  
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY  
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON ENERGY AND COMMERCE  
2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115  
Majority (201/225-2927)  
Minority (202/225-3631)  
March 22, 2016

Mr. Scott R. Peppet  
Professor of Law  
University of Colorado Law School  
420 Wolf Law Building, 401 UCB  
Boulder, CO 80309-0401

Dear Mr. Peppet,

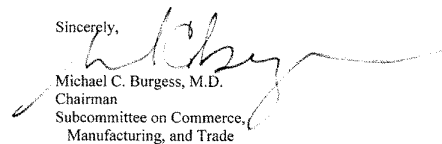
Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Thursday, March 3, 2016, to testify at the hearing entitled "Disrupter Series: Wearable Devices."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Tuesday, April 5, 2016. Your responses should be mailed to Giulia Giannangeli, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to [Giulia.Giannangeli@mail.house.gov](mailto:Giulia.Giannangeli@mail.house.gov).

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,



Michael C. Burgess, M.D.  
Chairman  
Subcommittee on Commerce,  
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

Attachment

[Mr. Peppet did not answer submitted questions for the record by the time of printing.]

FRED UPTON, MICHIGAN  
CHAIRMAN

FRANK PALLONE, JR., NEW JERSEY  
RANKING MEMBER

ONE HUNDRED FOURTEENTH CONGRESS  
**Congress of the United States**  
**House of Representatives**  
COMMITTEE ON ENERGY AND COMMERCE  
2125 RAYBURN HOUSE OFFICE BUILDING  
WASHINGTON, DC 20515-6115

Majority (202) 225-2927  
Minority (202) 225-3641

March 22, 2016

Mr. Doug Webster  
Vice President, Service Provider Marketing  
Cisco  
601 Pennsylvania Avenue, N.W., Suite 900  
Washington, DC 20004

Dear Mr. Webster,

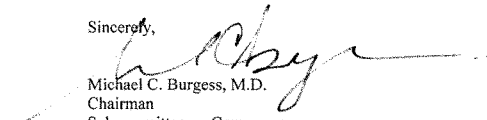
Thank you for appearing before the Subcommittee on Commerce, Manufacturing, and Trade on Thursday, March 3, 2016, to testify at the hearing entitled "Disrupter Series: Wearable Devices."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for ten business days to permit Members to submit additional questions for the record, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please respond to these questions by the close of business on Tuesday, April 5, 2016. Your responses should be mailed to Giulia Giannangeli, Legislative Clerk, Committee on Energy and Commerce, 2125 Rayburn House Office Building, Washington, DC 20515 and e-mailed in Word format to [Giulia.Giannangeli@mail.house.gov](mailto:Giulia.Giannangeli@mail.house.gov).

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

  
Michael C. Burgess, M.D.  
Chairman  
Subcommittee on Commerce,  
Manufacturing, and Trade

cc: Jan Schakowsky, Ranking Member, Subcommittee on Commerce, Manufacturing, and Trade

Attachment



Doug Webster, Vice President, Service Provider Marketing, Cisco

**Additional Questions for the Record – “Disruptor Series: Wearable Devices”**

**The Honorable Michael C. Burgess, M.D.**

**1) Mr. Webster, in what industry or industries do you see the most growth in use of wearable devices? And in what other industries do you expect to see that growth in the future?**

There are several industries where we can expect to see significant growth in the wearable devices market.

Presently, the **health care industry** is embracing the significant benefits that wearable devices can provide both to patients suffering from chronic medical conditions as well as healthy individuals who value preventative care. As mentioned in my testimony, examples include FDA-approved wearable devices that provide specific health issue monitoring, such as glucose or blood-sugar levels, which can be transmitted back to medical providers in real time. The changing face of healthcare will continue to be driven by devices that can track and analyze information about a person’s health.

Demand for new products in the **fitness industry** is also expected to continue to grow. Consumer demand has resulted in an influx of devices on the market which track statistics like heart rate, calories burned and steps taken.

**“Life-saving”** wearables is another area for major growth. These types of devices may include alarm or GPS-alerts, which offer personal security, or devices that could offer major benefits to the developing world, such as flood and earthquake warning wearables.

**Entertainment** is yet another industry which is on the cusp of a wearable technology breakthrough. Movie studios, game publishers, professional sports leagues and the music industry are developing virtual reality-embedded headsets, games, films, and apps to enhance the experience of their products and offerings.

There is no doubt the wearable market will continue to grow – and thrive - in these industries and many others.

**2) Mr. Webster, when you look at the development of wearable technology on a global scale, do you see anything different abroad than what is happening in the U.S. in terms of investment or innovation?**

Major technology companies around the globe are engaged in producing connected wearable devices. Countries such as Korea, Japan, China, the United States, Sweden and Finland are already large nodes for innovation and development of these technologies, with many other countries competing to join that top tier. The differences between international regions, to the extent differences develop, are likely to be in part a reflection of differences in approaches to consumer privacy. Highly prescriptive rules around privacy of consumer data from wearables raises the cost and difficulty for smaller entrepreneurial companies that may have a good idea but lack legal guidance to navigate these rules in order to bring that idea to reality.

If the full benefits of wearables are to be realized, the investment climate must be one in which good ideas can easily reach markets. Of course, regulations are necessary if there is a direct threat to human health or property. Government's role should be education – for example, encouraging digital literacy among consumers, transparency and privacy by design among developers, and enforcing against existing legal standards.

**3) What are the incentives for business and consumers who are not using wearables to start using wearables now?**

From a business perspective, there are significant market incentives to “get in on the action,” so to speak, both to address growing market opportunities or gain increased efficiencies, quality, or productivity. As highlighted in my testimony, we forecast approximately 600 million wearable devices globally by 2020, up from 97 million just last year. North America alone has a 40% market share of global wearable device connections as of today, with growth in Europe and Asia increasing each year. As with any burgeoning technology, the global business community does not want to miss the wave of consumer interest in this area.

Businesses simply cannot risk ignoring how wearable devices are disrupting industries. In customer facing industries, wearables may provide new methods for consumers to interface with service representatives, fostering customer loyalty and improved efficiency. This type of application can lead to significant cost savings, improved efficiencies, and much better customer experiences.

The incentives for consumers to start using wearable devices are also significant. Wearable devices can lead to improved safety, providing parents with an ability to keep track of their children. Wearables can also help consumers better manage their health and healthcare costs, improve their retail experiences, and assist with workplace productivity. The wearable market has endless potential to continue to improve the quality of life for consumers around the world.

**The Honorable Gregg Harper**

**1) What enhanced capabilities do you see wearable devices providing in the next five to 10 years, beyond what they are providing to consumers and businesses today?**

“The sky is the limit” when it comes to the potential capabilities of wearables in the future. Several products are currently in development that would enhance the benefits that businesses and consumers can gain from this type of technology.

Currently, wearable technology companies are developing biometric garments that can measure biometric data and activity levels, with a goal of notifying the user when it’s time to step away from the computer screen.

Other developments include wearables that converge with connected homes to drive efficiencies. For example, devices that could use an individual’s heartbeat signature to signal a door’s “smart” lock to unlock. This might be useful when you are returning home with groceries - or even an infant in hand. Another product currently in development can detect an individual’s core body temperature, then interacting with a Nest “smart” thermostat to trigger the air conditioning to turn on.

These are just a few examples of how the wearable market continues to innovate by making products that are more useful for consumers and businesses alike.

**2) What does this fast pace of innovation mean for policymakers in terms of how we should be thinking about the technology?**

Given the fast pace of innovation in this area, it is very important for policymakers to carefully consider the regulatory issues surrounding wearable devices.

As I highlighted in my testimony, there are four specific areas that legislators must consider as we look for public policies that encourage development in the wearable market.

First, policymakers need to ensure that radio spectrum is available with the right set of rules to make sure these devices can connect to the network.

Secondly, policymakers should support investment in the service provider networks that are needed to transport data to the Internet.

Third, a focus on policies that encourage start ups and small companies by ensuring access to venture capital, tax policies that support research & development, as well as encouraging more young people to enter careers in science, technology, engineering and math, also known as STEM.

And finally, these policies must ensure that device manufacturers and applications developers understand privacy and security threats, and take steps to protect their devices and the personal information of consumers.

Wearables represent a measurable component of the mobile landscape, and they are projected to continue to grow. They hold incredible promise to improve our lives. Public policies that encourage the development of this category should be supported so that the United States can continue to be a leader in this next chapter of the Internet.